

# AN ASYMPTOTIC FOR THE AVERAGE NUMBER OF AMICABLE PAIRS FOR ELLIPTIC CURVES

JAMES PARKS

with an appendix by Sumit Giri

**ABSTRACT.** Amicable pairs for a fixed elliptic curve defined over  $\mathbb{Q}$  were first considered by Silverman and Stange where they conjectured an order of magnitude for the function that counts such amicable pairs. This was later refined by Jones to give a precise asymptotic constant. The author previously proved an upper bound for the average number of amicable pairs over the family of all elliptic curves. In this paper we improve this result to an asymptotic for the average number of amicable pairs for a family of elliptic curves.

## 1. INTRODUCTION

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . For a prime  $p$ , let  $a_p(E)$  denote the trace of the Frobenius automorphism. Silverman and Stange [SS] define a pair  $(p, q)$  of prime numbers with  $p < q$  to be an *amicable pair* of  $E$  if  $E$  has good reduction at both  $p$  and  $q$  and

$$\#E_p(\mathbb{F}_p) := p + 1 - a_p(E_p) = q \quad \text{and} \quad \#E_q(\mathbb{F}_q) = p. \quad (1.1)$$

As observed in [SS, Remark 1.5] amicable pairs arose naturally when Silverman and Stange generalized Smyth's [Sm] results on index divisibility of Lucas sequences to elliptic divisibility sequences.

We are interested in the distribution of amicable pairs for a fixed elliptic curve  $E/\mathbb{Q}$ . We first define the amicable pair counting function, originally considered by Silverman and Stange [SS],

$$\pi_{E,2}(X) := \#\{p \leq X : \#E_p(\mathbb{F}_p) = q \text{ is prime and } \#E_q(\mathbb{F}_q) = p\}.$$

They used a heuristic argument to give the following conjecture for the behavior of  $\pi_{E,2}(X)$ .

**Conjecture 1.1 (Silverman-Stange).** *Let  $E/\mathbb{Q}$  be an elliptic curve. Assume that there are infinitely many primes  $p$  such that  $\#E_p(\mathbb{F}_p)$  is prime. Then as  $X \rightarrow \infty$  we have that*

$$\pi_{E,2}(X) \asymp \frac{\sqrt{X}}{(\log X)^2} \quad \text{if } E \text{ does not have complex multiplication (CM)}$$

and

$$\pi_{E,2}(X) \sim A_E \frac{X}{(\log X)^2} \quad \text{if } E \text{ has CM,}$$

where the implied constants in  $\asymp$  are both positive and depend only on  $E$  and  $A_E$  is a precise positive constant.

---

*Date:* January 26, 2016.

This work was supported by a Pacific Institute for the Mathematical Sciences Postdoctoral Fellowship.

**Remark 1.2.** (i) Silverman and Stange [SS] also defined an  $L$ -tuple  $(p_1, \dots, p_L)$  of distinct prime numbers to be an *aliquot cycle* of length  $L \geq 2$  of  $E$  if  $E$  has good reduction at each prime  $p_i$  and

$$\#E_{p_i}(\mathbb{F}_{p_i}) = p_{i+1} \text{ for } 1 \leq i \leq L-1 \text{ and } \#E_{p_L}(\mathbb{F}_{p_L}) = p_1.$$

They also introduced the analogously defined aliquot cycle counting function  $\pi_{E,L}(X)$ , and gave a conjecture for its behavior in the non-CM case. The main focus of their work was on aliquot cycles in the CM-case, where they proved that there are only finitely many under certain conditions when  $L \geq 3$  as well as showing that more structure occurs in the case  $L = 2$ .

Jones [J] refined Conjecture 1.1 in the non-CM case for aliquot cycles by using a heuristic argument similar to that of Lang and Trotter [LT]. We state the refined conjecture in the particular case of amicable pairs below.

**Conjecture 1.3 (Jones).** *Let  $E/\mathbb{Q}$  be an elliptic curve without complex multiplication. Then there is a non-negative real constant  $C_{E,2} \geq 0$  such that, as  $X \rightarrow \infty$ , we have that*

$$\pi_{E,2}(X) \sim C_{E,2} \int_2^X \frac{1}{2\sqrt{t}(\log t)^2} dt.$$

We note that the conjectured asymptotic is consistent with Conjecture 1.1. Moreover, Jones gave an explicit expression for the constant  $C_{E,2}$  in terms of invariants of the elliptic curve  $E$ . We discuss this constant in greater detail below.

For a non-zero integer  $n$ , we denote the  $n$ -torsion subgroup of  $E$  by  $E[n]$ . Let  $\mathbb{Q}(E[n])$  be the field generated by adjoining to  $\mathbb{Q}$  the  $x$  and  $y$ -coordinates of the  $n$ -torsion points of  $E$ . We have that  $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  for  $n \geq 2$ . Since each element of the Galois group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  acts on  $E[n]$  we have that  $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$  (see [Si, Chapter III.7]).

If  $[\text{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})] \leq 2$  for each  $n \geq 1$  then  $E$  is called a *Serre curve* (see [Se, pp. 309-311] and [LT, p. 51]). Jones [J] has shown that for any Serre curve  $E$  the conjectural constant  $C_{E,2}$  is positive and  $C_{E,2} = C_2 \cdot f_2(\Delta_{sf}(E))$ , where  $\Delta_{sf}(E)$  denotes the square-free part of the discriminant of any Weierstrass model of  $E$  and  $f_2$  is a positive function which approaches 1 as  $\Delta_{sf}(E) \rightarrow \infty$ . In particular, Jones [J] gave the formula

$$C_2 = \frac{8}{3\pi^2} \lim_{k \rightarrow \infty} \frac{n_k^2 \cdot \#\left\{(g_1, g_2) \in \text{GL}_2(\mathbb{Z}/n_k\mathbb{Z})^2 : \begin{array}{l} \det(g_2) \equiv \det(g_1) + 1 - \text{tr}(g_1) \pmod{n_k} \\ \det(g_1) \equiv \det(g_2) + 1 - \text{tr}(g_2) \pmod{n_k} \end{array} \right\}}{|\text{GL}_2(\mathbb{Z}/n_k\mathbb{Z})|^2}, \quad (1.2)$$

where  $n_k = \prod_{\ell \leq k} \ell^k$ .

There are currently no techniques known to approach conjectures like Conjecture 1.3 for a single elliptic curve. A much more tractable problem is to consider the behaviour of  $\pi_{E,2}(X)$  averaged over a family of elliptic curves. This approach has been used successfully to address many other problems related to distributions of invariants of elliptic curves. The most well known is the Lang-Trotter Conjecture [LT] which counts the number of primes  $p \leq X$  such that  $a_p(E) = t$  for a fixed integer  $t$ . The Lang-Trotter Conjecture was first shown to hold on average over a family of elliptic curves in the case  $t = 0$  by Fouvry and Murty [FM, Theorem 6] and then extended to the case of nonzero integers by David and Pappalardi [DP].

We let  $a$  and  $b$  be integers and let  $E_{a,b}$  be the elliptic curve given by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b,$$

with discriminant  $\Delta(E_{a,b}) \neq 0$ . For  $A, B > 0$  we consider the two parameter family of elliptic curves as

$$\mathcal{C} := \mathcal{C}(A, B) = \{E_{a,b} : |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0\}. \quad (1.3)$$

Conjecture 1.3 was considered on average in [P] over the family  $\mathcal{C}(A, B)$  in (1.3) where the conjectured upper bound for the average number of aliquot cycles with small bounds on the size of  $A$  and  $B$  was obtained (cf. [P, Theorem 1.6]). In this paper we extend this result to an asymptotic on average in the particular case of amicable pairs. We first state this result given in terms of a sum over primes.

**Theorem 1.4.** *Let  $\epsilon > 0$ , let  $E/\mathbb{Q}$  be an elliptic curve, and let  $\mathcal{C}$  be the family of elliptic curves in (1.3) with*

$$A, B > X^\epsilon \quad \text{and} \quad X^3(\log X)^6 < AB < e^{X^{\frac{1}{6}-\epsilon}}.$$

*Then we have that*

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,2}(X) = \frac{8}{3\pi^2} \sum_{p \leq X} \frac{C_2(p)}{\sqrt{p} \log p} + O\left(\frac{\sqrt{X}}{(\log X)^{2+\epsilon}}\right),$$

where

$$C_2(p) := \frac{4}{9} \prod_{\ell > 2} \left(1 - \frac{(2\ell^4 + 3\ell^3) \left(\frac{p-1}{\ell}\right)^2 + \ell^3 \left(\frac{p}{\ell}\right) - \ell^4 + 2\ell^3 + 4\ell^2 - 1}{(\ell^2 - 1)^3}\right). \quad (1.4)$$

In an appendix by Sumit Giri it will be shown that if we average the function  $C_2(p)$  defined in (1.4) over the set of primes up to  $X$  then we will obtain the constant  $C$  given in (1.6). Applying Theorem A.1 and partial summation we obtain the following result.

**Theorem 1.5.** *Under the same conditions as Theorem 1.4 we have that*

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,2}(X) = \frac{8C}{3\pi^2} \frac{\sqrt{X}}{(\log X)^2} + O\left(\frac{\sqrt{X}}{(\log X)^{2+\epsilon}}\right), \quad (1.5)$$

where

$$C := \prod_{\ell} \left(1 - \frac{(2\ell^4 + 3\ell^3)(\ell - 2) - (\ell - 1)(\ell^4 - 2\ell^3 - 4\ell^2 + 1)}{(\ell - 1)(\ell^2 - 1)^3}\right). \quad (1.6)$$

**Remark 1.6.** The average number of aliquot cycles, and in particular amicable pairs, has been independently studied by David, Koukoulopoulos and Smith [DKS, Theorem 1.6] using different techniques building upon a theorem of Gekeler [G, Theorem 5.5]. They also obtain an asymptotic result on average with an average constant expressed as

$$C' = \frac{8}{3\pi^2} \prod_{\ell} \lim_{k \rightarrow \infty} M(\ell, k)$$

where

$$M(\ell, k) := \frac{\ell^{2k} \cdot \#\left\{(\sigma_1, \sigma_2) \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 : \begin{array}{l} \det(\sigma_2) \equiv \det(\sigma_1) + 1 - \text{tr}(\sigma_1) \pmod{\ell^k} \\ \det(\sigma_1) \equiv \det(\sigma_2) + 1 - \text{tr}(\sigma_2) \pmod{\ell^k} \end{array} \right\}}{|GL_2(\mathbb{Z}/\ell^k\mathbb{Z})|^2}.$$

However, we note that the constant  $C$  is not an obvious consequence of the limit of  $M(\ell, k)$ .

**Remark 1.7.** Jones [J] also determined the Euler product representation of  $M(\ell, 1)$  which can be used to find the first approximation of  $C_2$ . However, it is not always the case that  $M(\ell, 1) = M(\ell, k)$  for  $k > 1$ <sup>1</sup>. In fact, for  $\ell > 2$  it is unclear if  $M(\ell, k)$  stabilizes at all.

The main result of this paper, Theorem 1.4, significantly improves [P, Theorem 3.1] in the case of amicable pairs, that is, when  $L = 2$  from an upper bound on average to an asymptotic result on average. The main tools used in this improvement are standard applications of Düring's theorem and the analytic class number formula along with a generalization of the approach of David and Smith [DS1], [DS2].

For an elliptic curve  $E/\mathbb{Q}$  and a fixed integer  $N$ , David and Smith [DS1], [DS2] and Chandee, David, Koukoulopoulos and Smith [CDKS] considered the related function that counts the number of primes  $p$  such that  $\#E_p(\mathbb{F}_p) = N$ . Many of the techniques used to sum class numbers in the proofs of [DS1, Theorem 3 and Theorem 7] as well as [CDKS, Proposition 5.1] generalize to the case of amicable pairs. However, the case of amicable pairs is more technical since we must now consider a sum of a product of class numbers.

**1.1. Acknowledgment.** This work was first started during my PhD under my advisor, Chantal David and I would like to thank her for all her great advice and insight while working on this problem. Also, I am extremely grateful to Amir Akbary for his encouragement and helpful intuition during the writing of this paper. I would also like to thank Sumit Giri for his careful reading and suggestions. Finally, I would like to thank Nathan Jones and Dimitris Koukoulopoulos for their very helpful discussions related to this paper.

## 2. PRELIMINARIES

We first fix notation. Throughout this paper we use  $\ell, p$ , and  $q$  to denote primes. For an elliptic curve  $E/\mathbb{Q}$ , we define the lower and upper limits of the Hasse bound as

$$p^- := p + 1 - 2\sqrt{p} < \#E_p(\mathbb{F}_p) < p^+ := p + 1 + 2\sqrt{p}. \quad (2.1)$$

Let  $n$  be a positive integer  $n$ . Then we let  $P^+(n)$  denote its largest prime factor and define  $\nu_\ell(n)$  to be the non-negative integer  $\alpha$  such that  $\ell^\alpha \parallel n$ . Let  $m$  be a positive integer, then we define  $\kappa_m(n)$  to be the multiplicative function defined on prime powers by

$$\kappa_m(\ell^{\nu_\ell(n)}) := \begin{cases} \ell & \text{if } 2 \nmid \nu_\ell(n) \text{ and } \ell \nmid m, \\ 1 & \text{otherwise.} \end{cases} \quad (2.2)$$

Let  $\chi_d$  be the real Dirichlet character given by the Kronecker symbol

$$\chi_d(n) := \left( \frac{d}{n} \right)$$

and associated Dirichlet series given by

$$L(s, \chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} = \prod_{\ell} \left( 1 - \frac{\chi_d(\ell)}{\ell^s} \right)^{-1} \quad \text{for } \Re(s) > 1.$$

Then for  $y > 1$  we define the truncated quadratic Dirichlet  $L$ -function as

$$L(1, \chi_d; y) := \prod_{\ell \leq y} \left( 1 - \frac{\chi_d(\ell)}{\ell} \right)^{-1}.$$

---

<sup>1</sup>For example,  $M(3, 1) \neq M(3, 2)$ .

We also make use of the notation

$$E(X, Y; q) := \max_{(a, q)=1} \left| \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q}}} \log p - \frac{Y}{\varphi(q)} \right|. \quad (2.3)$$

Lastly, for positive integers  $m$  and  $n$  we consider the symmetric function

$$D(m, n) := (m + 1 - n)^2 - 4m = D(n, m), \quad (2.4)$$

which occurs frequently in our calculations.

We require the following two technical results in the proofs of Theorem 1.4 and Proposition 3.2. The first proposition is a consequence of a result of Granville and Soundararajan [GS] which is essentially due to Elliot [E]. It allows us to bound the error terms in our calculations in Proposition 3.2.

**Proposition 2.1 (Granville-Soundararajan).** *Let  $\alpha \geq 1$  and  $Q \geq 3$ . There is a set  $\mathcal{E}_\alpha(Q) \subset [1, Q]$  of at most  $Q^{\frac{2}{\alpha}}$  integers such that if  $\chi$  is a Dirichlet character modulo  $q \leq \exp\{(\log Q)^2\}$ , whose conductor does not belong to  $\mathcal{E}_\alpha(Q)$ , then*

$$L(1, \chi) = L(1, \chi; (\log Q)^{8\alpha^2}) \left( 1 + O_\alpha \left( \frac{1}{(\log Q)^\alpha} \right) \right).$$

*Proof.* The result is stated in terms of primitive characters in [GS, Proposition 2.2]. The proof of the proposition in its present form is given in [CDKS, Lemma 2.3].  $\square$

The second result we require is the following version of the Bombieri-Vinogradov theorem for primes in short arithmetic progressions.

**Lemma 2.2 (Koukoulopoulos).** *Let  $\epsilon > 0$  and let  $A \geq 1$ . For  $2 \leq Y \leq X$  and  $1 \leq Q^2 \leq Y/X^{1/6+\epsilon}$ , we have that*

$$\int_X^{2X} \sum_{q \leq Q} E(u, Y; q) du \ll \frac{XY}{(\log X)^A}.$$

*Proof.* This result follows from [K, Theorem 1.1].  $\square$

We now state the analytic class number formula for quadratic Dirichlet  $L$ -functions (cf. [Da, Chapter 6]).

**Theorem 2.3.** *Let  $D = df^2$  be a negative number such that  $d$  is a negative fundamental discriminant and let  $\chi_d$  be the Kronecker symbol. Then*

$$\frac{h(d)}{w(d)} = \frac{\sqrt{-d}}{2\pi} L(1, \chi_d),$$

where  $h(d)$  denotes the usual class number of the imaginary quadratic order of discriminant  $d$  and  $w(d)$  is the number of roots of unity in  $\mathbb{Q}(\sqrt{d})$ .

We recall the following formulation of the definition of the Hurwitz-Kronecker class number (cf. [L]). Let  $D$  be a negative (not necessarily fundamental) discriminant. Then the *Hurwitz-Kronecker class number* of discriminant  $D$  is defined by

$$H(D) = \sum_{\substack{f^2 | D \\ \frac{D}{f^2} \equiv 0,1 \pmod{4}}} \frac{h\left(\frac{D}{f^2}\right)}{w\left(\frac{D}{f^2}\right)},$$

where  $w(D)$  is the number of roots of unity contained in  $\mathbb{Q}(\sqrt{D})$ . This formulation leads to the following useful result of Deuring [De].

**Theorem 2.4 (Deuring).** *Let  $p > 3$  be a prime and let  $t$  be an integer such that  $t^2 - 4p < 0$ . Then*

$$\sum_{\substack{\bar{E}/\mathbb{F}_p \\ a_p(\bar{E})=t}} \frac{1}{\#\text{Aut}(\bar{E})} = H(t^2 - 4p),$$

where  $\bar{E}$  denotes a representative of an isomorphism class of  $E/\mathbb{F}_p$ .

The following result [P, Theorem 3.1] allows us to interpret the average number of amicable pairs in terms of a sum of Hurwitz-Kronecker class numbers.

**Theorem 2.5.** *Let  $\epsilon > 0$ , let  $E/\mathbb{Q}$  be an elliptic curve, and let  $\mathcal{C}$  be the family of elliptic curves in (1.3) with*

$$A, B > X^\epsilon \quad \text{and} \quad X^3(\log X)^6 < AB < e^{X^{\frac{1}{6}-\epsilon}}.$$

Then as  $X \rightarrow \infty$  we have that

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,2}(X) = \left\{ \sum_{p \leq X} \frac{1}{p} \sum_{p^- < q < p^+} \frac{H(D(p,q))^2}{q} \right\} \left( 1 + O\left(\frac{1}{X^\epsilon}\right) \right). \quad (2.5)$$

In the analysis of the inner sum in (2.5) we require the following two lemmas.

**Lemma 2.6 (David-Smith).** *Let  $f, m, n$  be positive integers. Then*

$$\#\{m \in \mathbb{Z}/f\mathbb{Z} : D(m, n) \equiv 0 \pmod{f}\} \ll \sqrt{f}.$$

*Proof.* The proof is given in [DS1, Lemma 12].  $\square$

**Lemma 2.7 (David-Smith).** *Let  $p$  be a prime and let  $x$  be a positive real number. Then*

$$\sum_{n > x} \frac{1}{\kappa_{2p}(n)\varphi(n)} \ll \frac{1}{\sqrt{x}} \quad \text{and} \quad \sum_{n \geq 1} \frac{1}{\kappa_{2p}(n)\varphi(n)} \ll 1.$$

*Proof.* The result follows by specializing to the case where  $N$  is a prime in [DS1, Lemma 8].  $\square$

### 3. AN ASYMPTOTIC RESULT FOR A SUM OF A PRODUCT OF CLASS NUMBERS

The goal of this section is to first determine an asymptotic result for the inner sum in (2.5) and then to give the proof of the main result, Theorem 1.4.

**Theorem 3.1.** *Let  $\gamma > 0$ , let  $p, q$  be distinct primes, and let  $\epsilon > 0$ . Define  $Y := \frac{\sqrt{p}}{(\log p)^{\gamma+5}}$ , then we have that*

$$\begin{aligned} \sum_{p^- < q < p^+} \frac{H(D(p,q))^2}{q} &= \frac{8C_2(p)\sqrt{p}}{3\pi^2 \log p} + O\left(\frac{\sqrt{p}}{(\log p)^{1+\gamma}}\right. \\ &\quad \left. + \frac{1}{\log p} \sum_{\substack{-2\sqrt{p} < k \leq \frac{2\sqrt{p}}{Y} \\ f_1, f_2 \leq (\log 4p)^{32+8\gamma}}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(p+1+kY, Y; 4[n_1 f_2^2, n_2 f_2^2])\right), \end{aligned} \quad (3.1)$$

where  $C_2(p)$  is given in (1.4).

*Proof.* We first consider the left hand side of (3.1) and divide the interval  $(p^-, p^+)$  into intervals of length  $Y$ . We define these subintervals as

$$I := \left[ \frac{-2\sqrt{p}}{Y}, \frac{2\sqrt{p}}{Y} \right) \cap \mathbb{Z},$$

where for each  $k \in I$ , we write  $X_k := p + 1 + kY$ . Next we let  $d_i := D(p, q)/f_i^2$  for  $i = 1, 2$  and define

$$\chi_{d_1} := \left( \frac{D(p, q)/f_1^2}{\cdot} \right) \quad \text{and} \quad \chi_{d_2} := \left( \frac{D(p, q)/f_2^2}{\cdot} \right).$$

For  $p, q > 2$  we have that  $D(p, q)$  is odd and hence  $f_i$  is also odd for  $i = 1, 2$ . Therefore the condition  $D(p, q)/f_i^2 \equiv 1 \pmod{4}$  is always satisfied for  $i = 1, 2$ . Applying Theorem 2.3 gives

$$\begin{aligned} \sum_{p^- < q < p^+} \frac{H(D(p, q))^2}{q} &= \sum_{k \in I} \sum_{X_k < q \leq X_k + Y} \frac{H(D(p, q))^2}{q} \\ &= \frac{1}{4\pi^2} \sum_{k \in I} \sum_{X_k < q \leq X_k + Y} \frac{|D(p, q)|}{q} \sum_{f_1^2, f_2^2 | D(p, q)} \frac{L(1, \chi_{d_1}) L(1, \chi_{d_2})}{f_1 f_2} \\ &= \frac{1}{4\pi^2} \sum_{k \in I} \sum_{f_1, f_2 \leq \sqrt{X_k + Y}} \frac{1}{f_1 f_2} \sum_{\substack{X_k < q \leq X_k + Y \\ f_1^2, f_2^2 | D(p, q)}} \frac{|D(p, q)| L(1, \chi_{d_1}) L(1, \chi_{d_2})}{q}. \end{aligned} \tag{3.2}$$

We now focus on the inner sum of (3.2) and write

$$\frac{|D(p, q)|}{q} = \frac{|D(p, X_k)| \log q}{p \log p} + \left( \frac{|D(p, q)|}{q} - \frac{|D(p, X_k)| \log q}{p \log p} \right).$$

If  $q$  is a prime in the interval  $(X_k, X_k + Y]$ , then  $q = X_k + O(Y)$ , and hence  $D(p, q) = D(p, X_k) + O(Y\sqrt{p})$ . Since it is also true that  $q = p + O(\sqrt{p})$  we have that

$$\left| \frac{|D(p, q)|}{q} - \frac{|D(p, X_k)| \log q}{p \log p} \right| \ll \frac{|D(p, X_k)|}{p^{\frac{3}{2}}} + \frac{Y}{\sqrt{p}}.$$

Thus (3.2) becomes

$$\begin{aligned} &\sum_{p^- < q < p^+} \frac{H(D(p, q))^2}{q} \\ &= \frac{1}{4\pi^2 p \log p} \sum_{k \in I} |D(p, X_k)| \sum_{f_1, f_2 \leq \sqrt{X_k + Y}} \frac{1}{f_1 f_2} \sum_{\substack{X_k < q \leq X_k + Y \\ f_1^2, f_2^2 | D(p, q)}} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \log q \\ &+ O \left( \sum_{k \in I} \sum_{f_1, f_2 \leq \sqrt{X_k + Y}} \frac{1}{f_1 f_2} \sum_{\substack{X_k < q \leq X_k + Y \\ f_1^2, f_2^2 | D(p, q)}} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \left( \frac{|D(p, X_k)|}{p^{\frac{3}{2}}} + \frac{Y}{\sqrt{p}} \right) \right). \end{aligned} \tag{3.3}$$

By the convexity bound  $L(1, \chi_{d_i}) \ll \log |d_i| \ll \log p$  for  $i = 1, 2$  we have that the error term in (3.3) is bounded by

$$\frac{Y(\log p)^4}{p^{\frac{3}{2}}} \sum_{k \in I} |D(p, X_k)| + Y(\log p)^4. \quad (3.4)$$

Since  $D(p, X_k) = 0$  for  $k$  on the end points of the interval  $\left[\frac{-2\sqrt{p}}{Y}, \frac{2\sqrt{p}}{Y}\right] \supseteq I$ , we have by the Euler-MacLaurin summation formula that

$$\sum_{k \in I} |D(p, X_k)| = \int_{\frac{-2\sqrt{p}}{Y}}^{\frac{2\sqrt{p}}{Y}} (4p - (tY)^2) dt + O\left(\int_{\frac{-2\sqrt{p}}{Y}}^{\frac{2\sqrt{p}}{Y}} |t| Y^2 dt\right) = \frac{32p^{\frac{3}{2}}}{3Y} + O(p). \quad (3.5)$$

From (3.4) and (3.5) we have that the error term in (3.3) becomes  $O(Y^2(\log p)^4)$ . We then set  $X := X_k$  and define the inner sum in the main term of (3.3) as

$$S_1 := \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \log q. \quad (3.6)$$

We have the following technical result for the sum in (3.6). We delay the proof until Section 4.

**Proposition 3.2.** *Let  $\epsilon, \gamma > 0$ . Suppose that  $p^- < X < X + Y \leq p^+$  with  $Y \gg \frac{\sqrt{p}}{(\log p)^\nu}$  for  $\nu \geq 0$ . Then we have that*

$$\begin{aligned} \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \log q &= C_2(p)Y + O\left(\frac{Y}{(\log p)^\gamma}\right. \\ &\quad \left.+ \sum_{f_1, f_2 \leq (\log 4p)^{12+4\nu+4\gamma}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(X, Y; 4[n_1 f_2^2, n_2 f_2^2])\right), \end{aligned}$$

where  $C_2(p)$  is defined in (1.4).

The result now follows from applying Proposition 3.2 with  $\nu = 5 + \gamma$  and (3.5) to the main term in (3.3) and (3.4) and applying the fact that  $|D(p, X_k)| \ll p$  to the error terms.  $\square$

We now use Lemma 2.2 and Theorem 3.1 to prove the main result of this paper.

*Proof.* (Proof of Theorem 1.4) We first apply the result from Theorem 3.1 in Theorem 2.5, which gives

$$\begin{aligned} \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,2}(X) &= \frac{8}{3\pi^2} \sum_{p \leq X} \frac{C_2(p)}{\sqrt{p}(\log p)} (1 + O(X^{-\epsilon})) \\ &\quad + O\left(\sum_{p \leq X} \frac{1}{p \log p} \sum_{\frac{-2\sqrt{p}}{Y} < k \leq \frac{2\sqrt{p}}{Y}} \sum_{f_1, f_2 \leq (\log 4p)^{32+8\gamma}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(X_k, Y; 4[n_1 f_2^2, n_2 f_2^2])\right). \quad (3.7) \end{aligned}$$



Now the remainder of the proof is reduced to showing that

$$\sum_{p \leq X} \frac{1}{p \log p} \sum_{\frac{-2\sqrt{p}}{Y} < k \leq \frac{2\sqrt{p}}{Y}} \sum_{f_1, f_2 \leq (\log 4p)^{32+8\gamma}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(X_k, Y; 4[n_1 f_2^2, n_2 f_2^2]) \ll \frac{\sqrt{X}}{(\log X)^{2+\epsilon}}. \quad (3.8)$$

We first bound the inner sum in (3.8), which gives

$$\sum_{f_1, f_2 \leq (\log 4p)^{32+8\gamma}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(X_k, Y; 4[n_1 f_2^2, n_2 f_2^2]) \ll (\log 4p)^{64+16\gamma} \sum_{m \leq p^{3\epsilon}} E(X_k, Y; m).$$

Next we set

$$j := \frac{(p+1)}{Y} + k \quad \text{and} \quad f(p) := \frac{(\log p)^{63+16\gamma}}{p},$$

and by extending the sum over primes to a sum over all integers we have that the left hand side of (3.8) is bounded by

$$\sum_{p \leq X} f(p) \sum_{\frac{p^-}{Y} < j \leq \frac{p^+}{Y}} \sum_{m \leq p^{3\epsilon}} E(jY, Y; m) \leq \sum_{n \leq X} f(n) \sum_{\frac{n^-}{Y} < j \leq \frac{n^+}{Y}} \sum_{m \leq n^{3\epsilon}} E(jY, Y; m).$$

We break up the sum into dyadic intervals which gives

$$\begin{aligned} \sum_{\frac{X}{2} < n \leq X} f(n) \sum_{\frac{n^-}{Y} < j \leq \frac{n^+}{Y}} \sum_{m \leq n^{3\epsilon}} E(jY, Y; m) &\ll f(X) \sum_{m \leq X^{3\epsilon}} \sum_{j \asymp \frac{X}{Y}} E(jY, Y; m) \sum_{\substack{\frac{X}{2} < n \leq X \\ (jY)^- < n \leq (jY)^+}} 1 \\ &\ll f(X) \sqrt{X} \sum_{m \leq X^{3\epsilon}} \sum_{j \asymp \frac{X}{Y}} E(jY, Y; m) := E'. \end{aligned}$$

Let  $B > 0$  and set  $Y' := \frac{Y}{(\log X)^{B+4}}$ . Then we have that

$$\begin{aligned} E' &\ll f(X) \sqrt{X} \sum_{m \leq X^{3\epsilon}} \sum_{j \asymp \frac{X}{Y}} \left( \frac{1}{Y'} \int_{jY}^{jY+Y'} E(u, Y; m) du + \frac{Y'}{m} \right) \\ &\ll \frac{f(X) \sqrt{X}}{Y'} \sum_{m \leq X^{3\epsilon}} \int_{c_1 X}^{c_2 X} E(u, Y; m) du + \frac{f(X) X^{\frac{3}{2}}}{(\log X)^{B+3}}. \end{aligned} \quad (3.9)$$

The result follows by applying Lemma 2.2 to (3.9) with  $B = 62 + 17\gamma$  and  $A = 126 + 32\gamma$ .  $\square$

#### 4. PROOF OF PROPOSITION 3.2

In this section we give the proof of Proposition 3.2 stated in the previous section. Expanding upon the techniques of [DS1, Theorem 7] and [P, Proposition 3.2], we determine the coefficient of the main term for  $S_1$  in (3.6) as a function of  $p$ .

*Proof.* (Proof of Proposition 3.2) Recall from (3.6) that

$$S_1 := \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} L(1, \chi_{d_1}) L(1, \chi_{d_2}) \log q. \quad (4.1)$$

For the duration of this section let  $z := \log(4p)$  and let  $\alpha$  be a parameter  $\geq 10$ . Now let  $S'_1$  denote the double sum on the right hand side of (4.1) with  $L(1, \chi_{d_i}; z^{8\alpha^2})$  in place of  $L(1, \chi_{d_i})$  for  $i = 1, 2$ . We estimate the error term  $S_1 - S'_1$  by applying Proposition 2.1 with  $Q = 4p$ . We have that  $0 \leq -D(p, q) \leq 4p$  for  $q \in (p^-, p^+)$ . Moreover,  $\mathbb{Q}\left(\sqrt{\frac{D(p, q)}{f_i^2}}\right) = \mathbb{Q}(\sqrt{D(p, q)})$  and hence the conductor of  $\chi_{d_i}$  is equal to  $\text{disc}(\mathbb{Q}(\sqrt{D(p, q)}))$  for  $i = 1, 2$ . If  $\text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \notin \mathcal{E}_\alpha(4p)$  then by Proposition 2.1 and Mertens' theorem,

$$L(1, \chi_{d_1})L(1, \chi_{d_2}) - L(1, \chi_{d_1}; z^{8\alpha^2})L(1, \chi_{d_2}; z^{8\alpha^2}) \ll_\alpha \frac{(\log z)^2}{z^\alpha}.$$

If  $\text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \in \mathcal{E}_\alpha(4p)$  then for  $i = 1, 2$ , we use the convexity bound  $L(1, \chi_{d_i}) \ll \log p$ . In this case we have that

$$L(1, \chi_{d_1})L(1, \chi_{d_2}) - L(1, \chi_{d_1}; z^{8\alpha^2})L(1, \chi_{d_2}; z^{8\alpha^2}) \ll_\alpha z^2,$$

and thus

$$\begin{aligned} S_1 - S'_1 &\ll_\alpha \frac{(\log z)^2}{z^\alpha} \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q) \\ \text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \notin \mathcal{E}_\alpha(4p)}} \log q \\ &\quad + z^2 \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q) \\ \text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \in \mathcal{E}_\alpha(4p)}} \log q. \end{aligned}$$

For  $q \in (p^-, p^+)$  such that  $\Delta := \text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \in \mathcal{E}_\alpha(4p)$  we have that  $D(p, q) = \Delta m^2$  for some  $m \in \mathbb{N}$ . Equivalently  $(p+1-q)^2 - \Delta m^2 = 4p$ , where  $\Delta \equiv D(p, q) \equiv 1 \pmod{4}$ . Let  $n = p+1-q$ , then for a fixed  $\Delta \in \mathcal{E}_\alpha(4p)$  we need to determine the quantity

$$\begin{aligned} r(4p, 2) &:= \#\{(m, n) \in \mathbb{Z}^2 : n^2 - \Delta m^2 = 4p\}, \\ &= \#\left\{ \frac{n + m\sqrt{\Delta}}{2} \in \mathcal{O}_K : N\left(\frac{n + m\sqrt{\Delta}}{2}\right) = p \right\}, \end{aligned}$$

where  $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D(p, q)})$ ,  $\mathcal{O}_K$  is its ring of integers, and  $N(\cdot)$  is the norm of an element in  $K$ . Note that

$$\#\{I \subseteq \mathcal{O}_K : N(I) = d\} = \sum_{k|d} \left(\frac{\Delta}{k}\right),$$

where  $N(I)$  denotes the norm of an ideal  $I \subseteq \mathcal{O}_K$ . Thus,

$$\frac{r(4p, 2)}{6} \leq \#\{I \subseteq \mathcal{O}_K : N(I) = p\} = \sum_{k|p} \left(\frac{\Delta}{k}\right) \leq 2$$

and hence  $r(4p, 2) \leq 12$ . Since there are at most 12 admissible pairs  $(m, n)$  there are at most 12 admissible values of  $q$  since  $p$  is fixed. We have that  $\alpha \geq 10$ , and therefore from Proposition 2.1 we have that

$$\#\{p^- < q < p^+ : \text{disc}(\mathbb{Q}(\sqrt{D(p, q)})) \in \mathcal{E}_\alpha(4p)\} \leq 12\#\mathcal{E}_\alpha(4p) \ll p^{\frac{1}{5}}.$$

From the bound

$$\sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \log q \ll Y(\log p)^3, \quad (4.2)$$

we conclude that

$$S_1 - S'_1 \ll_{\alpha} \frac{(\log z)^2}{z^{\alpha}} Y(\log p)^3 + z^2 p^{\frac{1}{5}} (\log p)^3 \ll_{\alpha} Y \left( \frac{(\log p)^3 (\log \log 4p)^2}{(\log 4p)^{\alpha}} \right). \quad (4.3)$$

Let  $u \geq 1$  be a parameter to be determined later and for convenience let  $y := z^{8\alpha^2}$ . We have that

$$L(1, \chi; y) = \sum_{P^+(n) \leq y} \frac{\chi(n)}{n} = \sum_{\substack{P^+(n) \leq y \\ n \leq y^u}} \frac{\chi(n)}{n} + O \left( \sum_{\substack{P^+(n) \leq y \\ n > y^u}} \frac{1}{n} \right).$$

Note that for the error term above we have that

$$\begin{aligned} \sum_{\substack{P^+(n) \leq y \\ n > y^u}} \frac{1}{n} &\leq \frac{1}{e^u} \sum_{\substack{P^+(n) \leq y \\ n > y^u}} \frac{1}{n^{1-\frac{1}{\log y}}} \leq \frac{1}{e^u} \prod_{p \leq y} \left( 1 - \frac{1}{p^{1-\frac{1}{\log y}}} \right)^{-1} = \frac{1}{e^u} \prod_{p \leq y} \left( 1 - \frac{1}{p} + O \left( \frac{\log p}{p \log y} \right) \right)^{-1} \\ &\ll \frac{1}{e^u} \prod_{p \leq y} \left( 1 - \frac{1}{p} \right)^{-1} \prod_{p \leq y} \left( 1 + O \left( \frac{\log p}{(p-1) \log y} \right) \right)^{-1} \ll \frac{\log y}{e^u}, \end{aligned}$$

since the sum  $\sum_{p \leq y} \frac{\log p}{(p-1) \log y}$  converges. Then

$$L(1, \chi_{d_1}; y) L(1, \chi_{d_2}; y) = \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{\chi_{d_1}(n_1) \chi_{d_2}(n_2)}{n_1 n_2} + O \left( \frac{\log y}{e^u} \sum_{\substack{P^+(n) \leq y \\ n \leq y^u}} \frac{1}{n} + \frac{(\log y)^2}{e^{2u}} \right) \quad (4.4)$$

and by (4.2), (4.3) and (4.4), we have that (4.1) becomes

$$\begin{aligned} S_1 &= \sum_{f_1, f_2 \leq 2\sqrt{X+Y}} \frac{1}{f_1 f_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \log q \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{\chi_{d_1}(n_1) \chi_{d_2}(n_2)}{n_1 n_2} \\ &\quad + O_{\alpha} \left( \frac{Y(\log \log 4p)^2}{(\log p)^{\alpha-3}} + \frac{Y u (\log p)^3 (\log y)^2}{e^u} \right). \end{aligned} \quad (4.5)$$

Let  $V$  be a parameter to be determined later such that  $1 \leq V \leq 2\sqrt{X+Y}$ . We write the main term in (4.5) as

$$\begin{aligned} &\sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \chi_{d_1}(n_1) \chi_{d_2}(n_2) \log q + \left( \sum_{\substack{f_1 \leq V \\ V \leq f_2 \leq 2\sqrt{X+Y}}} \right. \\ &\quad \left. + \sum_{\substack{V < f_1 \leq 2\sqrt{X+Y} \\ f_2 \leq V}} + \sum_{V < f_1, f_2 \leq 2\sqrt{X+Y}} \right) \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \chi_{d_1}(n_1) \chi_{d_2}(n_2) \log q \\ &:= M_1 + E_1. \end{aligned} \quad (4.6)$$

From Lemma 2.6 and the definition of  $Y$  we have that the inner sum in  $E_1$  in (4.6) is

$$\begin{aligned}
& \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \chi_{d_1}(n_1) \chi_{d_2}(n_2) \log q \\
& \ll \log p \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{X < k \leq X+4\sqrt{p} \\ f_1, f_2 | D(p, k)}} 1 \\
& \ll (\log p) \sqrt{p} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{\#\{m \in \mathbb{Z}/[f_1, f_2]\mathbb{Z} : D(p, m) \equiv 0 \pmod{[f_1, f_2]}\}}{n_1 n_2 [f_1, f_2]} \\
& \ll \frac{\sqrt{p}(\log p) u^2 (\log y)^2}{\sqrt{[f_1, f_2]}}. \tag{4.7}
\end{aligned}$$

Hence, from (4.7) we have that

$$\begin{aligned}
E_1 & \ll \sqrt{p}(\log p) u^2 (\log y)^2 \left( \sum_{\substack{f_1 \leq V \\ V \leq f_2 \leq 2\sqrt{X+Y}}} + \sum_{\substack{V < f_1 \leq 2\sqrt{X+Y} \\ f_2 \leq V}} + \sum_{V < f_1, f_2 \leq 2\sqrt{X+Y}} \right) \frac{\sqrt{(f_1, f_2)}}{(f_1 f_2)^{\frac{3}{2}}} \\
& \ll \frac{\sqrt{p}(\log p) u^2 (\log y)^2}{V^{\frac{1}{4}}}, \tag{4.8}
\end{aligned}$$

by using the bound  $(f_1, f_2) \ll \sqrt{f_1 f_2}$ .

Combining the bounds from (4.8) and (4.6) with (4.5) gives

$$\begin{aligned}
S_1 &= \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{X < q \leq X+Y \\ f_1^2, f_2^2 | D(p, q)}} \chi_{d_1}(n_1) \chi_{d_2}(n_2) \log q \\
&+ O_\alpha \left( \frac{Y(\log \log 4p)^2}{(\log p)^{\alpha-3}} + \frac{Y u (\log p)^3 (\log y)^2}{e^u} + \frac{\sqrt{p}(\log p) u^2 (\log y)^2}{V^{\frac{1}{4}}} \right). \tag{4.9}
\end{aligned}$$

Then by quadratic reciprocity we have that the main term in (4.9) becomes

$$\begin{aligned}
& \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z} \\ a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left( \frac{a_1}{n_1} \right) \left( \frac{a_2}{n_2} \right) \sum_{\substack{X < q \leq X+Y \\ D(p, q) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p, q) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2}}} \log q \\
&= \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{n_1 n_2} \sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z} \\ a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left( \frac{a_1}{n_1} \right) \left( \frac{a_2}{n_2} \right) \\
&\times \left( \sum_{\substack{b \in (\mathbb{Z}/4[n_1 f_1^2, n_2 f_2^2]\mathbb{Z})^* \\ D(p, b) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p, b) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2}}} \sum_{\substack{X < q \leq X+Y \\ q \equiv b \pmod{4[n_1 f_1^2, n_2 f_2^2]}}} \log q + \sum_{\substack{X < q \leq X+Y \\ D(p, q) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p, q) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2} \\ q | 4[n_1 f_1^2, n_2 f_2^2]}} \log q \right). \tag{4.10}
\end{aligned}$$

Since  $q \neq 2$ , if  $q \mid 4[n_1 f_1^2, n_2 f_2^2]$  then either  $q \mid n_1 f_1^2$  or  $q \mid n_2 f_2^2$ . If  $q \mid n_1 f_1^2$  then since  $D(p, q) = q^2 - 2(p+1)q + (p-1)^2 \equiv a_1 f_1^2 \pmod{4n_1 f_1^2}$  then  $q \mid (4n_1 f_1^2, (p-1)^2 - a_1 f_1^2)$ . This implies that  $q \mid n_1(p-1)$ . Similarly, if  $q \mid n_2 f_2^2$  then  $q \mid n_2(p-1)$ . Thus, the second sum in (4.10) is bounded by

$$\begin{aligned} & \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{n_1, n_2 \leq y^u} \left( \sum_{q \mid n_1} \log q + \sum_{q \mid n_2} \log q + \sum_{q \mid p-1} \log q \right) \\ & \ll \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{n_1, n_2 \leq y^u} \log(n_1 n_2 (p-1)) \ll y^{2u} (\log V)^2 (u \log y + \log p). \end{aligned} \quad (4.11)$$

Let  $L := 4[n_1 f_1^2, n_2 f_2^2]$  then we replace the first inner sum in (4.10) by

$$\sum_{\substack{X < q \leq X+Y \\ q \equiv b \pmod{L}}} \log q := \frac{Y}{\varphi(L)} + \left( \sum_{\substack{X < q \leq X+Y \\ q \equiv b \pmod{L}}} \log q - \frac{Y}{\varphi(L)} \right).$$

If we fix  $b \in (\mathbb{Z}/L\mathbb{Z})^*$  there is at most one pair  $(a_1, a_2) \in \mathbb{Z}/4n_1\mathbb{Z} \times \mathbb{Z}/4n_2\mathbb{Z}$  such that  $D(p, b) \equiv a_i f_i^2 \pmod{4n_i f_i^2}$  for  $i = 1, 2$ . Hence, we have that

$$\begin{aligned} & \sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z} \\ a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left( \frac{a_1}{n_1} \right) \left( \frac{a_2}{n_2} \right) \sum_{\substack{b \in (\mathbb{Z}/L\mathbb{Z})^* \\ D(p, b) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p, b) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2}}} \left( \sum_{\substack{X < q \leq X+Y \\ q \equiv b \pmod{L}}} \log q - \frac{Y}{\varphi(L)} \right) \\ & \ll \sum_{b \in (\mathbb{Z}/L\mathbb{Z})^*} \left| \sum_{\substack{X < q \leq X+Y \\ q \equiv b \pmod{L}}} \log q - \frac{Y}{\varphi(L)} \right| \leq \varphi(L) E(X, Y; L), \end{aligned} \quad (4.12)$$

where the definition of  $E(X, Y; q)$  is given in (2.3). From (4.10), (4.11) and (4.12) we have that (4.9) becomes

$$\begin{aligned} S_1 = & Y \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1) \leq y \\ P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{1}{\varphi(L) n_1 n_2} \sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z} \\ a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left( \frac{a_1}{n_1} \right) \left( \frac{a_2}{n_2} \right) \sum_{\substack{b \in (\mathbb{Z}/L\mathbb{Z})^* \\ D(p, b) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p, b) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2}}} 1 \\ & + O_\alpha \left( \frac{Y (\log \log 4p)^2}{(\log p)^{\alpha-3}} + \frac{Y u (\log p)^3 (\log y)^2}{e^u} + \frac{\sqrt{p} (\log p) u^2 (\log y)^2}{V^{\frac{1}{4}}} \right. \\ & \left. + y^{2u} (\log V)^2 (u \log y + \log p) + \sum_{f_1, f_2 \leq V} f_1 f_2 \sum_{n_1, n_2 \leq y^u} E(X, Y; L) \right). \end{aligned} \quad (4.13)$$

Let  $\ell$  be a prime then by the Chinese remainder theorem we have that the inner sum in the main term of (4.13) becomes

$$\sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z} \\ a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left(\frac{a_1}{n_1}\right) \left(\frac{a_2}{n_2}\right) \prod_{\ell|L} \#\left\{m \in (\mathbb{Z}/\ell^{\nu_\ell(L)}\mathbb{Z})^* : D(p, m) \equiv a_1 f_1^2 \pmod{\ell^{\nu_\ell(4n_1 f_1^2)}} \text{ and } D(p, m) \equiv a_2 f_2^2 \pmod{\ell^{\nu_\ell(4n_2 f_2^2)}}\right\}. \quad (4.14)$$

Note that the set in the product of (4.14) is empty unless

$$a_1 f_1^2 \equiv a_2 f_2^2 \pmod{(4n_1 f_1^2, 4n_2 f_2^2)}.$$

For convenience, we give the notation,

$$(a, f, n) := \begin{cases} (a_1, f_1, n_1) & \text{if } \max\{\nu_\ell(4n_1 f_1^2), \nu_\ell(4n_2 f_2^2)\} = \nu_\ell(4n_1 f_1^2), \\ (a_2, f_2, n_2) & \text{if } \max\{\nu_\ell(4n_1 f_1^2), \nu_\ell(4n_2 f_2^2)\} = \nu_\ell(4n_2 f_2^2). \end{cases} \quad (4.15)$$

Then we write (4.14) as

$$\sum_{\substack{a_1 \in \mathbb{Z}/4n_1\mathbb{Z}, a_2 \in \mathbb{Z}/4n_2\mathbb{Z} \\ a_1 \equiv a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{(4n_1 f_1^2, 4n_2 f_2^2)}} \left(\frac{a_1}{n_1}\right) \left(\frac{a_2}{n_2}\right) \prod_{\ell|L} C_p^{(\ell)}(a, f, n), \quad (4.16)$$

where

$$C_p^{(\ell)}(a, f, n) := \#\{m \in (\mathbb{Z}/\ell^{\nu_\ell(4nf^2)}\mathbb{Z})^* : D(p, m) \equiv af^2 \pmod{\ell^{\nu_\ell(4nf^2)}}\}.$$

A more general version of the sum  $C_p^{(\ell)}(a, f, n)$  where  $p$  is any odd integer was first considered in [DS1]. Since we only consider when  $p$  is prime, we have the following special case of [DS1, Lemma 10].

**Lemma 4.1.** *Let  $p$  be an odd prime, let  $f$  be odd and let  $a \equiv 1 \pmod{4}$ . Let  $\ell$  be any odd prime dividing  $nf$ , and let  $e = \nu_\ell(4nf^2) = \nu_\ell(nf^2)$ . If  $\ell \nmid 4p + af^2$ , then*

$$C_p^{(\ell)}(a, f, n) = \begin{cases} 1 + \left(\frac{4p+af^2}{\ell}\right) & \text{if } \ell \nmid (p-1)^2 - af^2, \\ 1 & \text{if } \ell \mid (p-1)^2 - af^2. \end{cases}$$

If  $\ell \mid 4p + af^2$ , then, with  $s = \nu_\ell(4p + af^2)$ , we have

$$C_p^{(\ell)}(a, f, n) = \begin{cases} 2 \left(\frac{p+1}{\ell}\right)^2 \ell^{\frac{s}{2}} & \text{if } 1 \leq s < e, 2 \mid s, \text{ and } \left(\frac{(4p+af^2)/\ell^s}{\ell}\right) = 1, \\ \left(\frac{p+1}{\ell}\right)^2 \ell^{\lfloor e/2 \rfloor} & \text{if } s \geq e, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if  $\ell \mid f$ , then

$$C_p^{(\ell)}(a, f, n) := C_p^{(\ell)}(1, f, 1) = \begin{cases} 1 + \left(\frac{p(p-1)^2}{\ell}\right) & \text{if } \ell \neq p, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore,

$$C_p^{(2)}(a, f, n) = \begin{cases} 2 & \text{if } \nu_2(4nf^2) = 2 + \nu_2(n) = 2, \\ 4 & \text{if } \nu_2(4nf^2) = 2 + \nu_2(n) \geq 3 \text{ and } a \equiv 5 \pmod{8}, \\ 0 & \text{otherwise.} \end{cases}$$

Since  $C_p^{(2)}(a, f, n)$  does not depend on  $f$ , for convenience we define

$$S^{(2)}(a, n) := \frac{C_p^{(2)}(a, f, n)}{2} = \begin{cases} 1 & \text{if } 2 \nmid n, \\ 2 & \text{if } 2 \mid n \text{ and } a \equiv 5 \pmod{8}, \\ 0 & \text{otherwise.} \end{cases}$$

We now break up the product in (4.16) as

$$\prod_{\ell \mid L} C_p^{(\ell)}(a, f, n) = S^{(2)}(a, n) \prod_{\substack{\ell \mid n_1 n_2 \\ \ell \neq 2}} C_p^{(\ell)}(a, f, n) \prod_{\substack{\ell \mid f_1 f_2 \\ \ell \nmid n_1 n_2}} C_p^{(\ell)}(a, f, n). \quad (4.17)$$

Note that if  $\ell \mid f_1 f_2$  and  $\ell \nmid 2n_1 n_2$  then  $\max\{\nu_\ell(4n_1 f_1^2), \nu_\ell(4n_2 f_2^2)\} = \max\{\nu_\ell(f_1^2), \nu_\ell(f_2^2)\} > 0$  and hence

$$(a, f, n) = \begin{cases} (a_1, f_1, n_1) & \text{if } \max\{\nu_\ell(f_1^2), \nu_\ell(f_2^2)\} = \nu_\ell(f_1^2), \\ (a_2, f_2, n_2) & \text{if } \max\{\nu_\ell(f_1^2), \nu_\ell(f_2^2)\} = \nu_\ell(f_2^2). \end{cases}$$

From Lemma 4.1 and (4.17) we have that

$$\sum_{\substack{a_1 \in (\mathbb{Z}/4n_1\mathbb{Z})^* \\ a_2 \in (\mathbb{Z}/4n_2\mathbb{Z})^* \\ a_1 \equiv a_2 \equiv 1 \pmod{4}}} \left(\frac{a_1}{n_1}\right) \left(\frac{a_2}{n_2}\right) \sum_{\substack{b \in (\mathbb{Z}/L\mathbb{Z})^* \\ D(p,b) \equiv a_1 f_1^2 \pmod{4n_1 f_1^2} \\ D(p,b) \equiv a_2 f_2^2 \pmod{4n_2 f_2^2}}} 1 = 2C_{p,f}(n_1, n_2) \prod_{\substack{\ell \mid f_1 f_2 \\ \ell \nmid n_1 n_2}} C_p^{(\ell)}(1, f, 1), \quad (4.18)$$

where we define

$$C_{p,f}(n_1, n_2) := \sum_{\substack{a_1 \in (\mathbb{Z}/4n_1\mathbb{Z})^*, a_2 \in (\mathbb{Z}/4n_2\mathbb{Z})^* \\ a_1 \equiv a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{(4n_1 f_1^2, 4n_2 f_2^2)}} \left(\frac{a_1}{n_1}\right) \left(\frac{a_2}{n_2}\right) S^{(2)}(a, n) \prod_{\substack{\ell \mid n_1 n_2 \\ \ell \neq 2}} C_p^{(\ell)}(a, f, n). \quad (4.19)$$

Then from (4.18) we can express the main term of (4.13) as

$$\begin{aligned} & Y \sum_{f_1, f_2 \leq V} \frac{1}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\substack{\ell \mid f_1 f_2 \\ \ell \nmid n_1 n_2}} C_p^{(\ell)}(1, f, 1) \\ &= Y \sum'_{f_1, f_2 \leq V} \frac{\prod_{\ell \mid f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 \leq y^u}} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell \mid (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1}, \quad (4.20) \end{aligned}$$

where the prime on the sum over  $f_1$  and  $f_2$  indicates that the sums are to be restricted to those  $f_1, f_2$  such that  $C_p^{(\ell)}(1, f, 1) \neq 0$ . Now, we consider the size of  $C_{p,f}(n_1, n_2)$  in the following lemma. We delay the proof until Section 5.

**Lemma 4.2.** *Let  $p, f_1, f_2$ , and  $f$  be odd integers. Then the function  $C_{p,f}(n_1, n_2)$  is multiplicative in  $n_1, n_2$ . Let  $\alpha_1, \alpha_2$  be non-negative integers and let  $\ell$  be an odd prime. Then*

$$C_{p,f}(2^{\alpha_1}, 2^{\alpha_2}) = 2^{\max\{\alpha_1, \alpha_2\}} (-1)^{\alpha_1 + \alpha_2}.$$

*If  $\ell = p$  and  $\ell \nmid f_1 f_2$ , then*

$$C_{p,f}(p^{\alpha_1}, p^{\alpha_2}) = p^{\max\{\alpha_1, \alpha_2\} - 1} (p - 2).$$

*If  $\ell \nmid p f_1 f_2$ , then*

$$C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) = \ell^{\max\{\alpha_1, \alpha_2\} - 1} \begin{cases} \ell - 1 - \left(\frac{p}{\ell}\right) - \left(\frac{p-1}{\ell}\right)^2 & \text{if } 2 \mid \alpha_1 + \alpha_2, \\ -1 - \left(\frac{p-1}{\ell}\right)^2 & \text{if } 2 \nmid \alpha_1 + \alpha_2. \end{cases}$$

*If  $\ell \mid f_1 f_2$ , then*

$$\frac{C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})}{\ell^{\max\{\alpha_1, \alpha_2\} - 1}} = C_p^{(\ell)}(1, f, 1) \begin{cases} \ell - 1 & \text{if } \alpha_2 = 0, 2 \mid \alpha_1 \text{ and } \nu_\ell(f_1^2) \geq \nu_\ell(f_2^2), \\ \ell - 1 & \text{if } \alpha_1 = 0, 2 \mid \alpha_2 \text{ and } \nu_\ell(f_2^2) \geq \nu_\ell(f_1^2), \\ \ell - 1 & \text{if } \alpha_1 + \alpha_2 > 0, 2 \mid \alpha_1 + \alpha_2 \text{ and } \nu_\ell(f_1^2) = \nu_\ell(f_2^2), \\ 0 & \text{otherwise.} \end{cases}$$

*Furthermore, for any  $n_1, n_2$  we have the bound*

$$C_{p,f}(n_1, n_2) \ll \frac{n_1 n_2}{(n_1, n_2) \kappa_{2p}(n_1 n_2)} \prod_{\ell \mid (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1),$$

*where  $\kappa_{2p}(m)$  is defined in (2.2).*

The next step is to extend the sums in (4.20) to sums over all integers. We first focus on bounding the inner sum. We note that if  $((n_1, n_2), (f_1^2, f_2^2)) = 1$  then  $(n_1 f_1^2, n_2 f_2^2) = (n_1, n_2)(f_1^2, f_2^2)$ . Otherwise, there exists a prime  $\ell$  such that  $\ell \mid ((n_1, n_2), (f_1^2, f_2^2))$ . If  $C_{p,f}(\ell^{\nu_\ell(n_1)}, \ell^{\nu_\ell(n_2)}) \neq 0$  then from Lemma 4.2 either  $\nu_\ell(f_1^2) = \nu_\ell(f_2^2)$  or  $\ell \nmid (n_1, n_2)$  and thus  $(n_1 f_1^2, n_2 f_2^2) = (n_1, n_2)(f_1^2, f_2^2)$ . This gives the bound

$$\frac{1}{\varphi(L)} = \frac{(4n_1 f_1^2, 4n_2 f_2^2)}{\varphi(16n_1 n_2 f_1^2 f_2^2)} = \frac{(4n_1, 4n_2)(f_1^2, f_2^2)}{\varphi(16n_1 n_2 f_1^2 f_2^2)} \ll \frac{(n_1, n_2)(f_1^2, f_2^2)}{\varphi(n_1 n_2) \varphi(f_1^2) \varphi(f_2^2)}.$$

Hence, from Lemma 4.2 we have that

$$\frac{C_{p,f}(n_1, n_2)}{\varphi(L)} \ll \frac{n_1 n_2 (f_1^2, f_2^2)}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2) \varphi(f_1^2) \varphi(f_2^2)} \prod_{\ell \mid (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1). \quad (4.21)$$

From (4.21) we have that (4.20) becomes

$$\begin{aligned} & Y \sum'_{f_1, f_2 \leq V} \frac{\prod_{\ell \mid f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{P^+(n_1), P^+(n_2) \leq y} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L) n_1 n_2} \prod_{\ell \mid (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\ & + O \left( Y \sum'_{f_1, f_2 \leq V} \frac{(f_1^2, f_2^2) \prod_{\ell \mid f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2 \varphi(f_1^2) \varphi(f_2^2)} \left( \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1 \leq y^u, n_2 > y^u}} + \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1 > y^u, n_2 \leq y^u}} \right. \right. \\ & \left. \left. + \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 > y^u}} \right) \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} \right). \end{aligned} \quad (4.22)$$



We now consider the three inner sums in the error term of (4.22). Let  $d := (n_1, n_2)$  and write  $n_1 = dn'_1, n_2 = dn'_2$ . Since  $\nu_\ell(d^2 n'_1 n'_2) \equiv \nu_\ell(n'_1 n'_2) \pmod{2}$  we have that  $\kappa_{2p}(d^2 n'_1 n'_2) = \kappa_{2p}(n'_1 n'_2) = \kappa_{2p}(n'_1) \kappa_{2p}(n'_2)$ . Thus, breaking up the three inner sums in the error term in (4.22) into sums over  $d$  gives

$$\begin{aligned}
& \left( \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1 \leq y^u, n_2 > y^u}} + \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1 > y^u, n_2 \leq y^u}} + \sum_{\substack{P^+(n_1), P^+(n_2) \leq y \\ n_1, n_2 > y^u}} \right) \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} \\
& \leq \left( \sum_{d \leq y^u} \frac{1}{\varphi(d)^2} \sum_{\substack{n'_1 \leq \frac{y^u}{d} \\ n'_2 > \frac{y^u}{d}}} + \sum_{d \leq y^u} \frac{1}{\varphi(d)^2} \sum_{\substack{n'_1 > \frac{y^u}{d} \\ n'_2 \leq \frac{y^u}{d}}} + \sum_{d \geq 1} \frac{1}{\varphi(d)^2} \sum_{n'_1, n'_2 > \frac{y^u}{d}} \right) \frac{1}{\kappa_{2p}(n'_1) \kappa_{2p}(n'_2) \varphi(n'_1) \varphi(n'_2)} \\
& \leq \left( \sum_{d \leq y^u} \frac{1}{\varphi(d)^2} \sum_{\substack{n'_1 \leq \frac{y^u}{d} \\ n'_2 > \frac{y^u}{d}}} + \sum_{d \leq y^u} \frac{1}{\varphi(d)^2} \sum_{\substack{n'_1 > \frac{y^u}{d} \\ n'_2 \leq \frac{y^u}{d}}} \right) \frac{1}{\kappa_{2p}(n'_1) \kappa_{2p}(n'_2) \varphi(n'_1) \varphi(n'_2)} \\
& + \sum_{d \leq y^u} \frac{1}{\varphi(d)^2} \left( \sum_{n' > \frac{y^u}{d}} \frac{1}{\kappa_{2p}(n') \varphi(n')} \right)^2 + \sum_{d > y^u} \frac{1}{\varphi(d)^2} \left( \sum_{n' \geq 1} \frac{1}{\kappa_{2p}(n') \varphi(n')} \right)^2. \tag{4.23}
\end{aligned}$$

From Lemma 2.7 and partial summation we have that (4.23) is bounded by

$$\sum_{d \leq y^u} \left( \frac{1}{\varphi(d)^2} \frac{\sqrt{d}}{y^{\frac{u}{2}}} + \frac{1}{\varphi(d)^2} \frac{d}{y^u} \right) + \sum_{d > y^u} \frac{1}{\varphi(d)^2} \ll \frac{u(\log y)(\log \log y^u)^2}{y^u}.$$

By Lemma 4.1 there exists an  $\epsilon > 0$  such that

$$\prod_{\ell | f_1 f_2} C_p^{(\ell)}(1, f, 1) \ll \prod_{\ell | f_1 f_2} 2 = 2^{\omega(f_1 f_2)} \ll 2^{\frac{\log f_1 f_2}{\log \log f_1 f_2}} \ll f_1^\epsilon f_2^\epsilon,$$

where  $\omega(n)$  denotes the number of prime divisors of  $n$  and thus from (4.22) we have that (4.20) becomes

$$\begin{aligned}
& Y \sum'_{f_1, f_2 \leq V} \frac{\prod_{\ell | f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{\substack{P^+(n_1) \leq y \\ P^+(n_2) \leq y}} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell | (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\
& + O \left( Y \frac{u(\log y)(\log \log y^u)^2}{y^u} \right). \tag{4.24}
\end{aligned}$$

Now, as in (4.22) we write (4.24) as

$$\begin{aligned}
& \sum'_{f_1, f_2 \leq V} \frac{\prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{n_1, n_2 \geq 1} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell|(f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\
& + O\left(Y \sum'_{f_1, f_2 \leq V} \frac{(f_1^2, f_2^2) \prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2 \varphi(f_1^2) \varphi(f_2^2)} \left( \sum_{\substack{P^+(n_1) > y \\ P^+(n_2) \leq y}} + \sum_{\substack{P^+(n_1) \leq y \\ P^+(n_2) > y}} \right. \right. \\
& \left. \left. + \sum_{P^+(n_1), P^+(n_2) > y} \right) \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} + Y \frac{u(\log y)(\log \log y^u)^2}{y^u} \right). \tag{4.25}
\end{aligned}$$

Following analogously to (4.23) we have that the three inner sums in the error term in (4.25) are bounded by

$$\left( \sum_{\substack{P^+(n_1) > y \\ P^+(n_2) \leq y}} + \sum_{\substack{P^+(n_1) \leq y \\ P^+(n_2) > y}} + \sum_{P^+(n_1), P^+(n_2) > y} \right) \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} \ll \frac{1}{\sqrt{y}}. \tag{4.26}$$

Thus, from (4.26) we can write (4.25) as

$$\begin{aligned}
& Y \sum'_{f_1, f_2 \geq 1} \frac{\prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{n_1, n_2 \geq 1} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell|(f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\
& + O\left(Y \left( \sum_{\substack{f_1 \leq V \\ f_2 > V}} + \sum_{\substack{f_1 > V \\ f_2 \leq V}} + \sum_{f_1, f_2 > V} \right) \frac{(f_1^2, f_2^2) \prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2 \varphi(f_1^2) \varphi(f_2^2)} \sum_{n_1, n_2 \geq 1} \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} \right. \\
& \left. + Y \frac{(\log \log y^u)^2}{y^u} + \frac{Y}{\sqrt{y}} \right). \tag{4.27}
\end{aligned}$$

Following as above, we have that there exists an  $\epsilon > 0$  such that

$$\left( \sum_{\substack{f_1 \leq V \\ f_2 > V}} + \sum_{\substack{f_1 > V \\ f_2 \leq V}} + \sum_{f_1, f_2 > V} \right) \frac{(f_1^2, f_2^2) \prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2 \varphi(f_1^2) \varphi(f_2^2)} \sum_{n_1, n_2 \geq 1} \frac{1}{\kappa_{2p}(n_1 n_2) \varphi(n_1 n_2)} \ll \frac{(\log \log V)}{V^{1-\epsilon}}. \tag{4.28}$$

Combining (4.27) and (4.28) with (4.13) gives

$$\begin{aligned}
S_1 = & Y \sum'_{f_1, f_2 \geq 1} \frac{\prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{n_1, n_2 \geq 1} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell|(f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\
& + O_\alpha \left( \frac{Y(\log \log 4p)^2}{(\log 4p)^{\alpha-3}} + \frac{Y u(\log p)^3 (\log y)^2}{e^u} + \frac{\sqrt{p}(\log p) u^2 (\log y)^2}{V^{\frac{1}{4}}} + \frac{Y}{\sqrt{y}} + \frac{Y(\log \log V)}{V^{1-\epsilon}} \right. \\
& \left. + y^{2u} (\log V)^2 (u^2 (\log y)^2 + \log p) + \sum_{f_1, f_2 \leq V} f_1 f_2 \sum_{n_1, n_2 \leq y^u} E(X, Y; L) + \frac{Y(\log \log y^u)^2}{y^u} \right).
\end{aligned}$$

Choosing

$$V := (\log 4p)^{4\nu+4\gamma+12} \quad \text{and} \quad u := \frac{\log 4p}{(\log \log 4p)^2},$$

yields

$$\begin{aligned} S_1 = & Y \sum'_{f_1, f_2 \geq 1} \frac{\prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1)}{f_1 f_2} \sum_{n_1, n_2 \geq 1} \frac{2C_{p,f}(n_1, n_2)}{\varphi(L)n_1 n_2} \prod_{\ell|(f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1} \\ & + O_\alpha \left( \frac{Y}{(\log p)^\gamma} + \sum_{f_1, f_2 \leq (\log 4p)^{4\nu+4\gamma+12}} f_1 f_2 \sum_{n_1, n_2 \leq p^\epsilon} E(X, Y; L) \right). \end{aligned} \quad (4.29)$$

We now show that the sums in the main term of (4.29) converge. Recall that  $L = 4[n_1 f_1^2, n_2 f_2^2]$ . From the properties of the Euler  $\varphi$ -function we have that

$$\frac{1}{f_1 f_2} \frac{1}{n_1 n_2 \varphi(L)} = \frac{1}{f_1^2 \varphi(f_1) f_2^2 \varphi(f_2)} \frac{\varphi((n_1, f_1)) \varphi((n_2, f_2)) \varphi((4n_1 f_1^2, 4n_2 f_2^2))}{n_1 \varphi(4n_1) (n_1, f_1) n_2 \varphi(4n_2) (n_2, f_2)}.$$

To simplify our notation, we define the following multiplicative functions,

$$g_1(f_i) := \frac{1}{f_i^2 \varphi(f_i)} \quad \text{and} \quad g_2(n_i, f_i) := \frac{\varphi((n_i, f_i))}{n_i \varphi(4n_i) (n_i, f_i)} \quad \text{for } i = 1, 2.$$

Then we rewrite the main term of (4.29) as  $R(p)Y$  where

$$\begin{aligned} R(p) := & \sum'_{f_1, f_2 \geq 1} g_1(f_1) g_1(f_2) \prod_{\ell|f_1 f_2} C_p^{(\ell)}(1, f, 1) \sum_{n_1, n_2 \geq 1} 2g_2(n_1, f_1) g_2(n_2, f_2) \\ & \times \varphi((4n_1 f_1^2, 4n_2 f_2^2)) C_{p,f}(n_1, n_2) \prod_{\ell|(f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)^{-1}. \end{aligned} \quad (4.30)$$

Let  $n_1 := n'_1 n''_1, n_2 := n'_2 n''_2$ . Then we say that the function  $h(n_1, n_2)$  is *multiplicative* if  $h(n_1, n_2) = h(n'_1, n'_2) h(n''_1, n''_2)$  when  $(n'_1 n'_2, n''_1 n''_2) = 1$ . From Lemma 4.2 we have that the functions of  $n_1$  and  $n_2$  are multiplicative, so the sum over  $n_1, n_2$  in (4.30) becomes

$$\begin{aligned} & \varphi((f_1^2, f_2^2)) \left\{ 2 \sum_{\alpha_1, \alpha_2 \geq 0} g_2(2^{\alpha_1}, f_1) g_2(2^{\alpha_2}, f_2) \varphi((2^{2+\alpha_1}, 2^{2+\alpha_2})) C_{p,f}(2^{\alpha_1}, 2^{\alpha_2}) \right\} \\ & \times \left\{ 4 \sum_{\alpha_1, \alpha_2 \geq 0} g_2(p^{\alpha_1}, f_1) g_2(p^{\alpha_2}, f_2) \varphi((p^{\alpha_1}, p^{\alpha_2})) C_{p,f}(p^{\alpha_1}, p^{\alpha_2}) \right\} \\ & \times \prod_{\ell|2pf_1 f_2} \left\{ 4 \sum_{\alpha_1, \alpha_2 \geq 0} g_2(\ell^{\alpha_1}, f_1) g_2(\ell^{\alpha_2}, f_2) \varphi((\ell^{\alpha_1}, \ell^{\alpha_2})) C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) \right\} \\ & \times \prod_{\substack{\ell|f_1 f_2 \\ \ell \neq p}} \left\{ 1 + 4 \sum_{\substack{\alpha_1, \alpha_2 \geq 0 \\ \alpha_1 + \alpha_2 > 0}} g_2(\ell^{\alpha_1}, f_1) g_2(\ell^{\alpha_2}, f_2) \frac{\varphi((\ell^{\alpha_1} f_1^2, \ell^{\alpha_2} f_2^2)) C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})}{\varphi((f_1^2, f_2^2)) C_p^{(\ell)}(1, f, 1)} \right\}, \end{aligned} \quad (4.31)$$

by factoring out  $\varphi((f_1^2, f_2^2))$  from each product in (4.31).

We now invoke Lemma 4.2 and consider each term in (4.31) separately. For the first term we have that  $g_2(2^{\alpha_i}, f_i) = \frac{1}{2^{2\alpha_i+1}}$  for  $\alpha_i \geq 0$  and thus the first term in (4.31) becomes

$$1 + 2 \sum_{\alpha \geq 1} \left[ \frac{-1}{2} \right]^\alpha + \sum_{\alpha_1 \geq 1} \left[ \frac{-1}{2} \right]^{\alpha_1} \sum_{\alpha_2 \geq 1} \left[ \frac{-1}{2} \right]^{\alpha_2} = \frac{4}{9}. \quad (4.32)$$

For the second term we have that

$$g_2(p^{\alpha_i}, f_i) = \begin{cases} \frac{1}{2} & \text{if } \alpha_i = 0, \\ \frac{p}{2p^{2\alpha_i}(p-1)} & \text{if } \alpha_i > 0, \end{cases}$$

and thus the second sum in (4.31) becomes

$$1 + \frac{2(p-2)}{p-1} \sum_{\alpha \geq 1} \left[ \frac{1}{p} \right]^\alpha + \frac{p-2}{p-1} \sum_{\alpha_1 \geq 1} \left[ \frac{1}{p} \right]^{\alpha_1} \sum_{\alpha_2 \geq 1} \left[ \frac{1}{p} \right]^{\alpha_2} = 1 + \frac{(p-2)(2p-1)}{(p-1)^3}. \quad (4.33)$$

For the third sum, if  $\ell \nmid 2pf_1f_2$  then

$$g_2(\ell^{\alpha_i}, f_i) = \begin{cases} \frac{1}{2} & \text{if } \alpha_i = 0, \\ \frac{\ell}{2\ell^{2\alpha_i}(\ell-1)} & \text{if } \alpha_i > 0, \end{cases}$$

and thus the third sum in (4.31) becomes

$$\begin{aligned} & 1 + \frac{2}{\ell-1} \sum_{\alpha \geq 1} \left[ \frac{1}{\ell} \right]^\alpha \left[ -1 - \left( \frac{p-1}{\ell} \right)^2 + \left[ \ell - \left( \frac{p}{\ell} \right) \right] \left[ \frac{1 + (-1)^\alpha}{2} \right] \right] \\ & + \frac{1}{\ell-1} \sum_{\alpha_1 \geq 1} \left[ \frac{1}{\ell} \right]^{\alpha_1} \sum_{\alpha_2 \geq 1} \left[ \frac{1}{\ell} \right]^{\alpha_2} \left[ -1 - \left( \frac{p-1}{\ell} \right)^2 + \left[ \ell - \left( \frac{p}{\ell} \right) \right] \left[ \frac{1 + (-1)^{\alpha_1+\alpha_2}}{2} \right] \right] \\ & = 1 - \frac{(2\ell^3 + 3\ell^2 - 1) \left( \frac{p-1}{\ell} \right)^2 + (3\ell^2 - 1) \left( \frac{p}{\ell} \right) - \ell^3 + 3\ell^2 + \ell - 1}{(\ell-1)(\ell^2-1)^2}. \end{aligned} \quad (4.34)$$

For the fourth term, if  $\ell \mid f_1f_2$  then

$$g_2(\ell^{\alpha_i}, f_i) = \begin{cases} \frac{1}{2} & \text{if } \alpha_i = 0, \\ \frac{1}{2\ell^{2\alpha_i}} & \text{if } \alpha_i > 0, \end{cases}$$

and thus the last term in (4.31) becomes

$$1 + \sum_{\substack{\alpha_1, \alpha_2 \geq 0 \\ \alpha_1 + \alpha_2 > 0}} \left[ \frac{1}{\ell^2} \right]^{\alpha_1 + \alpha_2} \frac{\varphi((\ell^{\alpha_1} f_1^2, \ell^{\alpha_2} f_2^2)) C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})}{\varphi((f_1^2, f_2^2)) C_p^{(\ell)}(1, f, 1)}. \quad (4.35)$$

From Lemma 4.2, we must consider two cases. The first case is if  $\min\{\alpha_1, \alpha_2\} = 0$ , the second case is if  $\min\{\alpha_1, \alpha_2\} > 0$ . In the first case, if  $\nu_\ell(f_1^2) > \nu_\ell(f_2^2)$  then we have that  $(\ell^{\alpha_1} f_1^2, f_2^2) = (f_1^2, f_2^2)$  and similarly if  $\nu_\ell(f_2^2) > \nu_\ell(f_1^2)$  then  $(f_1^2, \ell^{\alpha_2} f_2^2) = (f_1^2, f_2^2)$ . Thus, in this case (4.35) becomes

$$1 + \frac{\ell-1}{2\ell} \sum_{\alpha \geq 1} \left[ \frac{1}{\ell} \right]^\alpha (1 + (-1)^\alpha) = 1 + \frac{1}{\ell(\ell+1)}.$$

If  $\nu_\ell(f_1^2) = \nu_\ell(f_2^2)$ , since  $\ell \mid f_1 f_2$ , when  $\alpha_1, \alpha_2 \geq 1$  we have that  $\varphi((\ell^{\alpha_1} f_1^2, \ell^{\alpha_2} f_2^2)) = \ell^{\min\{\alpha_1, \alpha_2\}} \varphi((f_1^2, f_2^2))$ . Hence, in this case (4.35) becomes

$$\begin{aligned} & 1 + \frac{\ell-1}{\ell} \sum_{\alpha \geq 1} \left[ \frac{1}{\ell} \right]^\alpha (1 + (-1)^\alpha) + \frac{\ell-1}{2\ell} \sum_{\alpha_1, \alpha_2 \geq 1} \left[ \frac{1}{\ell} \right]^{\alpha_1 + \alpha_2} (1 + (-1)^{\alpha_1 + \alpha_2}) \\ &= 1 + \frac{3\ell^2 - 1}{\ell(\ell-1)(\ell+1)^2}. \end{aligned}$$

By combining (4.32), (4.33), (4.34) and (4.35) we have that the sum over  $n_1, n_2$  in (4.30) becomes

$$\frac{4}{9} \varphi((f_1^2, f_2^2)) F_0(p) \prod_{\ell \nmid 2p f_1 f_2} F_1(\ell) \prod_{\substack{\ell \mid f_1 f_2 \\ \ell \neq p}} F_2(\ell, f_1, f_2), \quad (4.36)$$

where, for any odd prime  $\ell$ , we make the definitions

$$\begin{aligned} F_0(p) &:= 1 + \frac{(p-2)(2p-1)}{(p-1)^3}, \\ F_1(\ell) &:= 1 - \frac{(2\ell^3 + 3\ell^2 - 1) \left( \frac{p-1}{\ell} \right)^2 + (3\ell^2 - 1) \left( \frac{p}{\ell} \right) - \ell^3 + 3\ell^2 + \ell - 1}{(\ell-1)(\ell^2-1)^2}, \\ F_2(\ell, f_1, f_2) &:= \begin{cases} 1 + \frac{1}{\ell(\ell+1)} & \text{if } \nu_\ell(f_1^2) \neq \nu_\ell(f_2^2), \\ 1 + \frac{3\ell^2-1}{\ell(\ell-1)(\ell+1)^2} & \text{if } \nu_\ell(f_1^2) = \nu_\ell(f_2^2). \end{cases} \end{aligned}$$

Hence, (4.30) becomes

$$R(p) = \frac{4}{9} F_0(p) \prod_{\ell \neq 2, p} F_1(\ell) \sum'_{f_1, f_2 \geq 1} g_1(f_1) g_1(f_2) \varphi((f_1^2, f_2^2)) \prod_{\ell \mid f_1 f_2} C_p^{(\ell)}(1, f, 1) \frac{F_2(\ell, f_1, f_2)}{F_1(\ell)}. \quad (4.37)$$

We have that

$$g_1(\ell^{\alpha_i}) = \begin{cases} 1 & \text{if } \alpha_i = 0, \\ \frac{\ell}{\ell^{3\alpha_i}(\ell-1)} & \text{if } \alpha_i > 0, \end{cases}$$

so the sum in (4.37) over  $f_1, f_2$  may be factored as

$$\begin{aligned} & \prod_{\ell \neq 2, p} \left\{ 1 + \frac{\ell \left[ 1 + \left( \frac{p(p-1)^2}{\ell} \right) \right]}{(\ell-1)F_1(\ell)} \left[ \sum_{\alpha \geq 1} \left[ \frac{1}{\ell^3} \right]^\alpha (F_2(\ell, \ell^\alpha, 1) + F_2(\ell, 1, \ell^\alpha)) \right. \right. \\ & \quad \left. \left. + \sum_{\alpha_1 \geq 1} \left[ \frac{1}{\ell^3} \right]^{\alpha_1} \sum_{\alpha_2 \geq 1} \left[ \frac{1}{\ell^3} \right]^{\alpha_2} \ell^{2 \min\{\alpha_1, \alpha_2\}} F_2(\ell, \ell^{\alpha_1}, \ell^{\alpha_2}) \right] \right\} \\ &= \prod_{\ell \neq 2, p} \left\{ 1 + \frac{\left[ 1 + \left( \frac{p(p-1)^2}{\ell} \right) \right]}{F_1(\ell)} \left[ \frac{2\ell^3 + 3\ell^2 - \ell - 1}{(\ell^2 - 1)^3} \right] \right\}. \end{aligned} \quad (4.38)$$

Combining (4.34), (4.37) and (4.38) gives the equation

$$R(p) = \frac{4}{9}F_0(p) \prod_{\ell \neq 2, p} \left( 1 - \frac{(2\ell^4 + 3\ell^3) \left(\frac{p-1}{\ell}\right)^2 + \ell^3 \left(\frac{p}{\ell}\right) - \ell^4 + 2\ell^3 + 4\ell^2 - 1}{(\ell^2 - 1)^3} \right. \\ \left. + \frac{(2\ell^3 + 3\ell^2 - \ell - 1) \left(\left(\frac{p-1}{\ell}\right)^2 + \left(\frac{p}{\ell}\right) - 1 - \left(\frac{p(p-1)^2}{\ell}\right)\right)}{(\ell^2 - 1)^3} \right). \quad (4.39)$$

Note that since  $\ell \neq p$  we have that

$$\left(\frac{p-1}{\ell}\right)^2 + \left(\frac{p}{\ell}\right) - 1 - \left(\frac{p(p-1)^2}{\ell}\right) = 0,$$

and hence (4.39) becomes

$$R(p) = \frac{4}{9}F_0(p) \prod_{\ell \neq 2, p} \left( 1 - \frac{(2\ell^4 + 3\ell^3) \left(\frac{p-1}{\ell}\right)^2 + \ell^3 \left(\frac{p}{\ell}\right) - \ell^4 + 2\ell^3 + 4\ell^2 - 1}{(\ell^2 - 1)^3} \right).$$

Since

$$F_0(p) \left( 1 - \frac{2p^4 + 3p^3 - p^4 + 2p^3 + 4p^2 - 1}{(p^2 - 1)} \right)^{-1} = 1 + O\left(\frac{1}{p^2}\right),$$

we have that  $R(p) = C_2(p)(1 + O(p^{-2}))$  and the result follows.  $\square$

## 5. PROOF OF LEMMA 4.2

We now provide the proof of Lemma 4.2 stated in the previous section. The function  $C_{p,f}(n_1, n_2)$  is very similar to the function  $C_{N,f}(n)$  considered in [DS1, Lemma 11] and we will make frequent reference to their paper in the following proof. For the duration of this section let  $a_1, a_2, f_1, f_2, n_1, n_2$  be integers such that  $f_1$  and  $f_2$  are odd and recall that  $L = 4[n_1 f_1^2, n_2 f_2^2]$ .

*Proof.* (Proof of Lemma 4.2) We first show that  $C_{p,f}(n_1, n_2)$  is multiplicative in two variables. Let  $n_1 := n'_1 n''_1, n_2 := n'_2 n''_2$ . Recall the function  $C_{p,f}(n_1, n_2)$  is multiplicative if  $C_{p,f}(n_1, n_2) = C_{p,f}(n'_1, n'_2) C_{p,f}(n''_1, n''_2)$  when  $(n'_1 n'_2, n''_1 n''_2) = 1$  and  $C_{p,f}(1, 1) = 1$ .

Define  $(a', f, n')$  and  $(a'', f, n'')$  analogously to (4.15). Now, suppose that  $(n'_1 n'_2, n''_1 n''_2) = 1$ , then we can assume that at least one of  $n'_1 n'_2$  and  $n''_1 n''_2$  is odd. Without loss of generality, we assume that  $n'_1 n'_2$  is odd and hence  $n'$  is also odd. Therefore there exist integers  $h'_1, h''_1, h'_2, h''_2, h', h''$  such that

$$4n''_1 h''_1 + n'_1 h'_1 = 4n''_2 h''_2 + n'_2 h'_2 = 4n'' h'' + n' h' = 1. \quad (5.1)$$

Since we assumed that  $n'_1 n'_2$  is odd, we have that  $S^{(2)}(a', n') = 1$  and by definition,

$$\begin{aligned}
 & C_{p,f}(n'_1, n'_2) C_{p,f}(n''_1, n''_2) \\
 &= \sum_{\substack{a'_1 \in (\mathbb{Z}/n'_1 \mathbb{Z})^* \\ a'_1 \equiv 1 \pmod{4}}} \left( \frac{a'_1}{n'_1} \right) \sum_{\substack{a'_2 \in (\mathbb{Z}/n'_2 \mathbb{Z})^* \\ a'_1 f_1^2 \equiv a'_2 f_2^2 \pmod{(4n'_1 f_1^2, 4n'_2 f_2^2)}}} \left( \frac{a'_2}{n'_2} \right) \prod_{\substack{\ell | n'_1 n'_2 \\ \ell \neq 2}} C_p^{(\ell)}(a', f, n') \\
 &\times \sum_{\substack{a''_1 \in (\mathbb{Z}/4n''_1 \mathbb{Z})^* \\ a''_1 \equiv 1 \pmod{4}}} \left( \frac{a''_1}{n''_1} \right) \sum_{\substack{a''_2 \in (\mathbb{Z}/4n''_2 \mathbb{Z})^* \\ a''_2 \equiv 1 \pmod{4} \\ a''_1 f_1^2 \equiv a''_2 f_2^2 \pmod{(4n''_1 f_1^2, 4n''_2 f_2^2)}}} \left( \frac{a''_2}{n''_2} \right) S^{(2)}(a'', n'') \prod_{\ell | n''_1 n''_2} C_p^{(\ell)}(a'', f, n''). \quad (5.2)
 \end{aligned}$$

From (5.1) we have that  $a'_1 = a'_1(4n''_1 h''_1 + n'_1 h'_1)$ , and hence

$$\left( \frac{a'_1}{n'_1} \right) = \left( \frac{a'_1(4n''_1 h''_1 + n'_1 h'_1)}{n'_1} \right) = \left( \frac{a'_1 4n''_1 h''_1}{n'_1} \right) = \left( \frac{a'_1 4n''_1 h''_1 + a''_1 n'_1 h'_1}{n'_1} \right).$$

Similarly, we have that

$$\left( \frac{a''_1}{n''_1} \right) = \left( \frac{a'_1 4n''_1 h''_1 + a''_1 n'_1 h'_1}{n''_1} \right),$$

and the analogous results for  $a'_2$  and  $a''_2$ .

We assumed that  $(n', n'') = 1$  and we have that  $n'_1 \equiv n'_2 \equiv 0 \pmod{(4n'_1 f_1^2, 4n'_2 f_2^2)}$ . Thus,

$$\begin{aligned}
 a'_1 f_1^2 &= a'_1(4n''_1 h''_1 + n'_1 h'_1) f_1^2 \equiv (a'_1 4n''_1 h''_1) f_1^2 \equiv (a'_1 4n''_1 h''_1 + a''_1 n'_1 h'_1) f_1^2 \\
 &\equiv (a'_2 4n''_2 h''_2 + a''_2 n'_2 h'_2) f_2^2 \pmod{(4n'_1 n''_1 f_1^2, 4n'_2 n''_2 f_2^2)}.
 \end{aligned}$$

Hence, the right hand side of (5.2) becomes

$$\begin{aligned}
 & \sum_{\substack{a'_1 \in (\mathbb{Z}/n'_1 \mathbb{Z})^* \\ a''_1 \in (\mathbb{Z}/4n''_1 \mathbb{Z})^* \\ a''_1 \equiv 1 \pmod{4}}} \left( \frac{a'_1 4n''_1 h''_1 + a''_1 n'_1 h'_1}{n'_1 n''_1} \right) \sum_{\substack{a'_2 \in (\mathbb{Z}/n'_2 \mathbb{Z})^*, a''_2 \in (\mathbb{Z}/4n''_2 \mathbb{Z})^* \\ a''_2 \equiv 1 \pmod{4} \\ (a'_1 4n''_1 h''_1 + a''_1 n'_1 h'_1) f_1^2 \equiv (a'_2 4n''_2 h''_2 + a''_2 n'_2 h'_2) f_2^2 \pmod{(4n'_1 n''_1 f_1^2, 4n'_2 n''_2 f_2^2)}}} \left( \frac{a'_2}{n'_2} \right) \\
 &\times \left( \frac{a'_2 4n''_2 h''_2 + a''_2 n'_2 h'_2}{n'_2 n''_2} \right) S^{(2)}(a' 4n'' h'' + a'' n' h', f, n' n'') \prod_{\ell | n'_1 n'_2 n''_1 n''_2} C_p^{(\ell)}(a' 4n'' h'' + a'' n' h', f, n' n'') \\
 &= C_{p,f}(n'_1 n''_1, n'_2 n''_2),
 \end{aligned}$$

and thus  $C_{p,f}(n_1, n_2)$  is multiplicative.

Now let  $\alpha_i := \nu_\ell(n_i)$  for  $i = 1, 2$  and consider the sum  $C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})$ . Without loss of generality it suffices to consider the case when  $(a, f, n) = (a_1, f_1, \ell^{\alpha_1})$  since  $C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})$  is symmetric.

We first consider  $C_{p,f}(2^{\alpha_1}, 2^{\alpha_2})$ , when  $\alpha_1 \geq 1$  and  $\alpha_1 \geq \alpha_2$ . From Lemma 4.1 we have that

$$\begin{aligned}
 C_{p,f}(2^{\alpha_1}, 2^{\alpha_2}) &= 2 \sum_{\substack{a_1 \in (\mathbb{Z}/2^{\alpha_1+2} \mathbb{Z})^* \\ a_1 \equiv 5 \pmod{8}}} \left( \frac{a_1}{2^{\alpha_1}} \right) \sum_{\substack{a_2 \in (\mathbb{Z}/2^{\alpha_2+2} \mathbb{Z})^* \\ a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{2^{2+\alpha_2}(f_1^2, f_2^2)}}} \left( \frac{a_2}{2^{\alpha_2}} \right) \\
 &= 2 \sum_{\substack{a_1 \in (\mathbb{Z}/2^{\alpha_1+2} \mathbb{Z})^* \\ a_1 \equiv 5 \pmod{8}}} \left( \frac{a_1}{2} \right)^{\alpha_1 + \alpha_2} = 2^{\alpha_1} \sum_{\substack{a_1 \in (\mathbb{Z}/8 \mathbb{Z})^* \\ a_1 \equiv 5 \pmod{8}}} \left( \frac{a_1}{2} \right)^{\alpha_1 + \alpha_2} = 2^{\alpha_1} (-1)^{\alpha_1 + \alpha_2}.
 \end{aligned}$$

Next we consider when  $\ell \nmid 2f_1f_2$ . In this case,

$$C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) = \sum_{\substack{a_1 \in (\mathbb{Z}/4\ell^{\alpha_1}\mathbb{Z})^* \\ a_1 \equiv 1 \pmod{4}}} \left( \frac{a_1}{\ell^{\alpha_1}} \right) C_p^{(\ell)}(a_1, f_1, \ell^{\alpha_1}) \sum_{\substack{a_2 \in (\mathbb{Z}/4\ell^{\alpha_2}\mathbb{Z})^* \\ a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{4(f_1^2, f_2^2)\ell^{\alpha_2}}}} \left( \frac{a_2}{\ell^{\alpha_2}} \right).$$

Since  $\ell \nmid f_1f_2$ , we have that the inner sum above becomes

$$\sum_{\substack{a_2 \in (\mathbb{Z}/4\ell^{\alpha_2}\mathbb{Z})^* \\ a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{\ell^{\alpha_2}}}} \left( \frac{a_2}{\ell^{\alpha_2}} \right) = \left( \frac{a_1}{\ell} \right)^{\alpha_2},$$

and hence

$$C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) = \sum_{\substack{a_1 \in (\mathbb{Z}/4\ell^{\alpha_1}\mathbb{Z})^* \\ a_1 \equiv 1 \pmod{4}}} \left( \frac{a_1}{\ell} \right)^{\alpha_1 + \alpha_2} C_p^{(\ell)}(a_1, f_1, \ell^{\alpha_1}). \quad (5.3)$$

We have that the sum in (5.3) differs only by the exponent on the Legendre symbol from the quantity  $C_{N,f}(\ell^\alpha)$  considered in [DS1, Equation (38)]. It follows that their method can be applied analogously to obtain the formula for  $C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2})$  in the case  $\ell \nmid 2f_1f_2$  given in the statement of the lemma.

It remains to consider the case when  $\ell \mid f_1f_2$ . We assumed that  $(a, f, n) = (a_1, f_1, \ell^{\alpha_1})$ , and therefore  $(4\ell^{\alpha_1}f_1^2, 4\ell^{\alpha_2}f_2^2) = 4\ell^{\alpha_2 + \nu_\ell(f_2^2)}(f_1^2/\ell^{\nu_\ell(f_1^2)}, f_2^2/\ell^{\nu_\ell(f_2^2)})$  and in this case

$$\begin{aligned} C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) &= C_p^{(\ell)}(1, f, 1) \sum_{\substack{a_1 \in (\mathbb{Z}/4\ell^{\alpha_1}\mathbb{Z})^* \\ a_1 \equiv 1 \pmod{4}}} \left( \frac{a_1}{\ell^{\alpha_1}} \right) \sum_{\substack{a_2 \in (\mathbb{Z}/4\ell^{\alpha_2}\mathbb{Z})^* \\ a_2 \equiv 1 \pmod{4} \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{4\ell^{\alpha_2 + \nu_\ell(f_2^2)}(f_1^2/\ell^{\nu_\ell(f_1^2)}, f_2^2/\ell^{\nu_\ell(f_2^2)})}}} \left( \frac{a_2}{\ell^{\alpha_2}} \right) \\ &= C_p^{(\ell)}(1, f, 1) \sum_{a_1 \in (\mathbb{Z}/\ell^{\alpha_1}\mathbb{Z})^*} \left( \frac{a_1}{\ell^{\alpha_1}} \right) \sum_{\substack{a_2 \in (\mathbb{Z}/\ell^{\alpha_2}\mathbb{Z})^* \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{\ell^{\alpha_2 + \nu_\ell(f_2^2)}}}} \left( \frac{a_2}{\ell^{\alpha_2}} \right). \end{aligned} \quad (5.4)$$

If  $\alpha_2 = 0$ , since  $a_2 f_2^2 \equiv 0 \pmod{\ell^{\nu_\ell(f_2^2)}}$ , for a solution to exist we must have that  $a_1 f_1^2 \equiv 0 \pmod{\ell^{\nu_\ell(f_2^2)}}$  as well. Thus, we require that  $\nu_\ell(f_2^2) \leq \nu_\ell(f_1^2)$ . This gives

$$\begin{aligned} C_{p,f}(\ell^{\alpha_1}, 1) &= C_p^{(\ell)}(1, f, 1) \sum_{a_1 \in (\mathbb{Z}/\ell^{\alpha_1}\mathbb{Z})^*} \left( \frac{a_1}{\ell^{\alpha_1}} \right) = C_p^{(\ell)}(1, f, 1) \ell^{\alpha_1 - 1} \sum_{a_1 \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left( \frac{a_1}{\ell} \right)^{\alpha_1} \\ &= C_p^{(\ell)}(1, f, 1) \ell^{\alpha_1 - 1} \begin{cases} \ell - 1 & \text{if } 2 \mid \alpha_1 \text{ and } \nu_\ell(f_2^2) \leq \nu_\ell(f_1^2), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If  $\alpha_2 \geq 1$  then  $a_1 f_1^2 \equiv a_2 f_2^2 \pmod{\ell^{\alpha_2 + \nu_\ell(f_2^2)}}$  has a solution if and only if  $(a_2 f_2^2, \ell^{\alpha_2 + \nu_\ell(f_2^2)}) = \ell^{\nu_\ell(f_2^2)} \mid a_1 f_1^2$ . Thus, we require that  $\nu_\ell(f_2^2) \leq \nu_\ell(f_1^2)$ . Now define integers  $h_1$  and  $h_2$  such



that  $f_1^2 = h_1^2 \ell^{\nu_\ell(f_1^2)}$ ,  $f_2^2 = h_2^2 \ell^{\nu_\ell(f_2^2)}$  and  $(h_1 h_2, \ell) = 1$ . Then the sum over  $a_2$  in (5.4) becomes

$$\begin{aligned} \sum_{\substack{a_2 \in (\mathbb{Z}/\ell^{\alpha_2} \mathbb{Z})^* \\ a_1 f_1^2 \equiv a_2 f_2^2 \pmod{\ell^{\alpha_2 + \nu_\ell(f_2^2)}}}} \left( \frac{a_2}{\ell} \right)^{\alpha_2} &= \sum_{\substack{a_2 \in (\mathbb{Z}/\ell^{\alpha_2} \mathbb{Z})^* \\ a_2 \equiv a_1 h_1^2 (h_2^2)^{-1} \ell^{\nu_\ell(f_1^2) - \nu_\ell(f_2^2)} \pmod{\ell^{\alpha_2}}}} \left( \frac{a_2}{\ell} \right)^{\alpha_2} \\ &= \left( \frac{a_1 \ell^{\nu_\ell(f_1^2) - \nu_\ell(f_2^2)}}{\ell} \right)^{\alpha_2} = \left( \frac{\ell^{\nu_\ell(f_1^2) - \nu_\ell(f_2^2)}}{\ell} \right) \left( \frac{a_1}{\ell} \right)^{\alpha_2}. \end{aligned}$$

Then in this case we have that

$$\begin{aligned} C_{p,f}(\ell^{\alpha_1}, \ell^{\alpha_2}) &= \left( \frac{\ell^{\nu_\ell(f_1^2) - \nu_\ell(f_2^2)}}{\ell} \right) C_p^{(\ell)}(1, f, 1) \sum_{a_1 \in (\mathbb{Z}/\ell^{\alpha_1} \mathbb{Z})^*} \left( \frac{a_1}{\ell} \right)^{\alpha_1 + \alpha_2} \\ &= C_p^{(\ell)}(1, f, 1) \ell^{\alpha_1 - 1} \begin{cases} \ell - 1 & \text{if } 2 \mid \alpha_1 + \alpha_2 \text{ and } \nu_\ell(f_1^2) = \nu_\ell(f_2^2), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Since  $C_{p,f}(n_1, n_2)$  is multiplicative, we have for a prime  $\ell$  that

$$C_{p,f}(n_1, n_2) = \prod_{\ell \mid n_1 n_2} C_{p,f}(\ell^{\nu_\ell(n_1)}, \ell^{\nu_\ell(n_2)}).$$

Then it follows from the above results that

$$C_{p,f}(\ell^{\nu_\ell(n_1)}, \ell^{\nu_\ell(n_2)}) \ll \left( \frac{\ell^{\nu_\ell(n_1) + \nu_\ell(n_2)}}{(\ell^{\nu_\ell(n_1)}, \ell^{\nu_\ell(n_2)}) \kappa_{2p}(\ell^{\nu_\ell(n_1) + \nu_\ell(n_2)})} \right) \prod_{\ell \mid (f_1 f_2, n_1 n_2)} C_p^{(\ell)}(1, f, 1)$$

with an absolute constant. The result follows by taking the product over  $\ell \mid n_1 n_2$ .  $\square$

## APPENDIX A. BY SUMIT GIRI

The goal of this appendix is to determine the average of the function  $C_2(p)$ , defined in (1.4), over the set of primes up to  $X$ . We state this result as follows.

**Theorem A.1.** *Let  $C_2(p)$  be the constant defined in (1.4). Then for any  $M > 0$ , we have*

$$\sum_{p \leq X} C_2(p) = C \pi(X) \left( 1 + O \left( \frac{1}{(\log X)^M} \right) \right),$$

where  $C$  is given by

$$C := \prod_{\ell} \left( 1 - \frac{(2\ell^4 + 3\ell^3)(\ell - 2) - (\ell - 1)(\ell^4 - 2\ell^3 - 4\ell^2 + 1)}{(\ell - 1)(\ell^2 - 1)^3} \right).$$

*Proof.* First recall the function

$$C_2(p) := \frac{4}{9} \prod_{\ell > 2} \left( 1 - \frac{(2\ell^4 + 3\ell^3) \left( \frac{p-1}{\ell} \right)^2 + \ell^3 \left( \frac{p}{\ell} \right) - \ell^4 + 2\ell^3 + 4\ell^2 - 1}{(\ell^2 - 1)^3} \right).$$

For each prime  $p$ , we define the function  $f_p(\ell)$  by

$$f_p(\ell) := (2\ell^4 + 3\ell^3) \left( \frac{p-1}{\ell} \right)^2 + \ell^3 \left( \frac{p}{\ell} \right) - \ell^4 + 2\ell^3 + 4\ell^2 - 1.$$

Then

$$\sum_{p \leq X} C_2(p) = \sum_{p \leq X} \sum_{\substack{n \geq 1 \\ n \text{ odd}}} (-1)^{\omega(n)} \frac{\mu^2(n)}{n^2} \prod_{\ell|n} \left( \frac{f_p(\ell) \ell^2}{(\ell^2 - 1)^3} \right) \quad (\text{A.1})$$

where  $\omega(n)$  is the number of distinct prime factors of  $n$  and  $\mu(n)$  is the Möbius function. In (A.1) we restrict the inner sum to integers  $n \leq (\log X)^M$ , which gives rise to an error term of size  $X/(\log X)^B$ . Thus, the main term in (A.1) becomes

$$\sum_{\substack{1 \leq n \leq (\log X)^M \\ n \text{ odd}}} (-1)^{\omega(n)} \mu^2(n) \prod_{\ell|n} \frac{1}{(\ell^2 - 1)^3} \sum_{p \leq X} \prod_{\ell|n} f_p(\ell). \quad (\text{A.2})$$

Now we define three multiplicative functions  $a(\cdot)$ ,  $b(\cdot)$ , and  $c(\cdot)$ , supported on square-free integers by

$$a(\ell) = 2\ell^4 + 3\ell^3, \quad b(\ell) = \ell^3, \quad c(\ell) = 2\ell^3 - \ell^4 + 4\ell^2 - 1. \quad (\text{A.3})$$

In other words,  $f_p(\ell) = a(\ell) \left(\frac{p-1}{\ell}\right)^2 + b(\ell) \left(\frac{p}{\ell}\right) + c(\ell)$  if  $\ell$  is prime. For every odd integer  $n$ , we have

$$\begin{aligned} \sum_{p \leq X} \prod_{\ell|n} f_p(\ell) &= \sum_{p \leq X} \sum_{\substack{n_1 n_2 n_3 = n \\ (n_1, n_2) = (n_2, n_3) = (n_3, n_1) = 1}} a(n_1) \left(\frac{p-1}{n_1}\right)^2 b(n_2) \left(\frac{p}{n_2}\right) c(n_3) \\ &= \sum_{\substack{n_1 n_2 n_3 = n \\ (n_1, n_2) = (n_2, n_3) = (n_3, n_1) = 1}} a(n_1) b(n_2) c(n_3) \sum_{\substack{p \leq X \\ (p-1, n_1) = 1}} \left(\frac{p}{n_2}\right) \\ &= \sum_{\substack{n_1 n_2 n_3 = n \\ (n_1, n_2) = (n_2, n_3) = (n_3, n_1) = 1}} a(n_1) b(n_2) c(n_3) \sum_{b \in (\mathbb{Z}/n_2\mathbb{Z})^*} \left(\frac{b}{n_2}\right) \sum_{\substack{p \leq X \\ p \equiv b \pmod{n_2} \\ (p-1, n_1) = 1}} 1. \end{aligned} \quad (\text{A.4})$$

We now consider the multiplicative function

$$\delta(m) := \#\{1 \leq a \leq m-1 : (a, m) = (a+1, m) = 1\}.$$

Then, using the Siegel–Walfisz theorem for modulus  $n_1 n_2 \leq (\log X)^M$ , the last sum in (A.4) is equal to  $\frac{\delta(n_1) \text{Li}(X)}{\phi(n_1 n_2)}$  with an error term  $E(X)$ , bounded by  $X \cdot \exp(-c(\log X)^{\frac{1}{2}})$  for some constant  $c$ . Note that since  $n \leq (\log X)^M$ , the error term  $E(X)$  does not affect the size of the error term in the statement of the theorem.

Finally, the main term in (A.4) is then equal

$$\text{Li}(X) \sum_{\substack{n_1 n_2 n_3 = n \\ (n_1, n_2) = (n_2, n_3) = (n_3, n_1) = 1}} \frac{\delta(n_1) a(n_1) b(n_2) c(n_3)}{\phi(n_1 n_2)} \sum_{b \in (\mathbb{Z}/n_2\mathbb{Z})^*} \left(\frac{b}{n_2}\right).$$

We have that the last sum in the above expression is zero if  $n_2 \geq 3$ . Also since  $n$  is odd, the only contribution comes from the trivial case  $n_2 = 1$ .

In that case, (A.2) becomes

$$\pi(X) \sum_{\substack{n \geq 1 \\ n \text{ odd}}} (-1)^{\omega(n)} \mu^2(n) \prod_{\ell|n} \frac{1}{(\ell^2 - 1)^3} \sum_{\substack{n_1 n_3 = n \\ (n_3, n_1) = 1}} \frac{\delta(n_1) a(n_1) c(n_3)}{\phi(n_1)} + O\left(\frac{X}{(\log X)^{M+1}}\right). \quad (\text{A.5})$$

We have that the function inside the outer sum in the main term in (A.5) is multiplicative in  $n$ , and hence can be written as the Euler product

$$\prod_{\ell > 2} \left( 1 - \frac{(a(\ell)\delta(\ell)/\phi(\ell)) + c(\ell)}{(\ell^2 - 1)^3} \right).$$

Then the result follows from the fact that  $\delta(\ell) = (\ell - 2)$ . This completes the proof.  $\square$

## REFERENCES

- [CDKS] V. Chandee, C. David, D. Koukoulopoulos and E. Smith, The frequency of elliptic curves over prime finite fields. preprint, arXiv:1405.6923.
- [Da] H. Davenport, *Multiplicative Number Theory*. Third edition. Revised and with a preface by Hugh L. Montgomery. *Graduate Texts in Mathematics*, 74, Springer-Verlag, New York, 2000.
- [DKS] C. David, D. Koukoulopoulos and E. Smith, Sums of Euler products and statistics of elliptic curves preprint.
- [DP] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices* 1999, no. 4, 165–183.
- [DS1] C. David and E. Smith, Elliptic curves with a given number of points over finite fields. *Compos. Math.* 149 (2013), no. 2, 175–203.
- [DS2] C. David and E. Smith, Corrigendum to: Elliptic curves with a given number of points over finite fields. *Compos. Math.* 150 (2014), no. 8, 1347–1348.
- [De] M. Deuring, Die Typen der Multiplikatorringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14 (1941), no. 1, 197–272.
- [E] P. Elliott, On the size of  $L(1, \chi)$ , *J. reine angew. Math.* 236 (1969), 2636.
- [FM] E. Fouvry and M. R. Murty, On the distribution of supersingular primes. *Canad. J. Math.* 48 (1996), no. 1, 81–104.
- [G] E. Gekeler, Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, 2003, no. 37, 1999–2018.
- [GS] A. Granville and K. Soundararajan, The distribution of values of  $L(1, \chi_d)$ . *Geom. Funct. Anal.*, 13 (2003), no. 5, 992–1028.
- [J] N. Jones, Elliptic aliquot cycles of fixed length. *Pacific J. Math.* 263 (2013), no. 2, 353–371.
- [K] D. Koukoulopoulos, Primes in short arithmetic progressions. *Int. J. Number Theory* (to appear).
- [LT] S. Lang and H. Trotter, *Frobenius distributions in  $GL_2$ -extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976.
- [L] H. Lenstra, Factoring integers with elliptic curves. *Ann. of Math.* (2) 126 (1987), no. 3, 649–673.
- [P] J. Parks, Amicable pairs and aliquot cycles on average. *Int. J. Number Theory* 11 (2015), no. 6, 1751–1790.
- [Se] J-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.
- [Si] J. Silverman, *The arithmetic of elliptic curves*, *Graduate Texts in Mathematics*, 106 Springer-Verlag, New York, 1986.
- [SS] J. Silverman and K. Stange, Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.* 20 (2011), no. 3, 329–357.
- [Sm] C. Smyth, The terms in Lucas sequences divisible by their indices. *J. Integer Seq.* 13 (2010), no. 2, Article 10.2.4, 18 pp.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE,  
 4401 UNIVERSITY DRIVE, LETHBRIDGE, AB, T1K 3M4, CANADA  
*Present address:* INSTITUT FÜR ALGEBRA, ZAHLENTHEORIE UND DISKRETE MATHEMATIK,  
 LEIBNIZ UNIVERSITÄT HANNOVER, WELFENGARTEN 1, 30167 HANNOVER, GERMANY  
*E-mail address:* parks@math.uni-hannover.de